

Brian Kabala
4920 Holly Grove Drive
Las Vegas, Nevada 89130

FILED	RECEIVED
ENTERED	SERVED ON
COUNSEL/PARTIES OF RECORD	
<div style="border: 1px solid black; padding: 5px; margin: 5px auto; width: 150px;"> MAR 13 2017 </div>	
CLERK US DISTRICT COURT DISTRICT OF NEVADA	
BY: _____	DEPUTY _____

**UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA**

LHF PRODUCTIONS, INC,

PLAINTIFF,

VS.

AGUSTIN BERTOLIN, an individual; MARIA
GONZALEZ, an individual; BRIAN KABALA, an
individual; JOHN KOEHL, an individual;
DANIEL O'CONNELL, an individual; DONALD
PLAIN, an individual; DAVID POOR, an individual;
ANTE SODA, an individual; MATTHEW
STEWART, an individual; AARON TAKAHASHI,
an individual; and JOHN AND JANE DOES, 1-10

Defendants

CASE NO.: 2:16-CV-02028

**DEFENDANT KABALA'S FIRST AMENDED
COMPLAINT ANSWER AND AFFRIMATIVE
DEFENSES; AND COUNTERCLAIM**

Defendant Brian Kabala ("Defendant") hereby submits their Answer, Affirmative Defenses and Counterclaim to Plaintiff's First Amended Complaint ("Complaint").

NATURE OF THE ACTION

1. Lacks information to respond.
2. Part (a) denied as to this defendant. Part (b) denied.

JURISDICTION AND VENUE

3. Lacks information to respond.

1 4. Denied in part. Defendant did not commit copyright infringement or tortious conduct as
2 started in the body or part (a). Defendant admits paying for internet as stated in part (b),
3 but this does not prove the defendant was responsible for copyright infringement.

4 5. Part (a) denies the inference this defendant committed copyright infringement. Part (b)
5 admitted as to this defendant. Lacks information to respond on the rest.

6 **PARTIES**

7 6. Admitted.

8 7. Lacks information to respond.

9 8. Lacks information to respond.

10 9. Part (c) is admitted, but this does not prove the defendant was responsible for copyright
11 infringement. Lacks information to respond on the rest.

12 **JOINDER**

13 10. Denied in its entirety.

14 **FACTUAL BACKGROUND**

15 **I. The Plaintiff Owns the Copyright to the Motion Picture**

16 11. Lacks information to respond.

17 13. Lacks information to respond. (Paragraph 12 noted as missing)

18 **II. The Defendants Used BitTorrent To Infringe the Plaintiff's Copyright**

19 14. Lacks information to respond.

20 15. Lacks information to respond.

21 **A. Each Defendant Installed a BitTorrent Client onto his or her Computer.**

22 16. Denied as to this defendant.

23 17. Lacks information to respond.

24 18. Lacks information to respond.

25 **B. The Initial Seed, Torrent, Hash and Tracker**

26 19. Lacks information to respond.

27 20. Lacks information to respond.

28 21. Lacks information to respond.

1 22. Lacks information to respond.

2 23. Lacks information to respond.

3 24. Lacks information to respond.

4 25. Denies the inference this defendant committed copyright infringement. Lacks information
5 to respond on the rest.

6 26. Lacks information to respond.

7 **C. Torrent Sites**

8 27. Lacks information to respond.

9 28. Denied as to this defendant.

10 **D. Uploading and Downloading a Work through a BitTorrent Swarm**

11 29. Denies the inference this defendant committed copyright infringement. Lacks information
12 to respond on the rest.

13 30. Denies the inference this defendant committed copyright infringement. Lacks information
14 to respond on the rest.

15 31. Denies the inference this defendant committed copyright infringement. Lacks information
16 to respond on the rest.

17 32. Denies the inference this defendant committed copyright infringement. Lacks information
18 to respond on the rest.

19 33. Denied.

20 34. Denies the inference this defendant committed copyright infringement. Lacks information
21 to respond on the rest.

22 35. Denied as to this defendant.

23 **E. The Plaintiff's Computer Investigators Identified Each of the Defendants' IP**

24 **Addresses as Participants in a Swarm That Was Distributing the Plaintiff's**

25 **Copyrighted Work.**

26 36. Denies the inference this defendant committed copyright infringement. Lacks information
27 to respond on the rest.

28 37. Lacks information to respond.

38. Lacks information to respond.

39. Lacks information to respond on the first portion, with the exception of "and show:", which

refers to the following statements: Part (A) denied as to this defendant. Part (B) denied.

Plaintiff has submitted no evidence to prove their allegation in Part (B). The evidence

would have to at least show that each defendant was connected at the same time, which

'Summary of Defendants' IP Address Data' (Dkt. No. 1, Exhibit 1) expressly does not.

This is why the plaintiff's allegations of contributory infringement are baseless.

40. Denied as to this defendant.

41. Lacks information to respond.

42. Lacks information to respond.

MISCELLANEOUS

43. Denied as to this defendant committing copyright infringement.

44. Lacks information to respond.

FIRST CLAIM FOR RELIEF (Direct Copyright Infringement)

45. Defendant reaffirms his denial of all allegations in the foregoing paragraphs.

46. Lacks information to respond.

47. Denied as to this defendant.

48. Denied.

49. Denied as to this defendant in its entirety.

50. Denied as to this defendant.

51. Denied as to this defendant.

52. Denied as to this defendant.

SECOND CLAIM FOR RELIEF (Contributory Copyright Infringement)

53. Defendant reaffirms his denial of all allegations in the foregoing paragraphs.

54. Lacks information to respond.

55. Denied as to this defendant committing copyright infringement.

56. Denied.

1 57. Denied.

2 58. Denied.

3 59. Denied.

4 60. Denied.

5 61. Denied.

6 62. Denied as to this defendant directly infringing. Denies the notion of secondary
7 infringement as to all defendants.

8 63. Denied as to this defendant directly infringing. Denies the notion of secondary
9 infringement as to all defendants.

10 **THIRD CLAIM FOR RELIEF**
11 (Vicarious Copyright Infringement)

12 64. Defendant reaffirms his denial of all allegations in the foregoing paragraphs.

13 65. Lacks information to respond.

14 66. Denied.

15 67. (First Paragraph 67) Admitted as to this defendant.

16 67. (Second Paragraph 67) Admitted in part. Defendant uses an internet connection, but this
17 does not prove the defendant is responsible for copyright infringement. Denies the notion
18 of secondary infringement as to all defendants.

19 68. (First Paragraph 68) Denied.

20 68. (Second Paragraph 68) Denied as to this defendant directly infringing. Denies the notion
21 of secondary infringement as to all defendants.

22 69. Denied as to this defendant directly infringing. Denies the notion of secondary
23 infringement as to all defendants.

24 **DEMAND FOR A JURY TRIAL**

25 Defendant hereby relies on Plaintiff's demand for a jury trial in connection with its complaint.

26 **AFFIRMATIVE DEFENSES**

27 Having answered the Complaint, the Defendant asserts the following enumerated
28 Affirmative defenses:

I. FIRST DEFENSE
(Comparative Negligence)

The Defendant asserts that Plaintiff's alleged damages were caused, in part, as a result of Plaintiff's own negligence, therefore, Plaintiff's recovery should be proportionally diminished by the Doctrine of Comparative Negligence.

II. SECOND DEFENSE
(Failure to Mitigate Damages)

The Defendant asserts that the Plaintiff failed to mitigate any damages allegedly sustained. Accordingly, any damages actually sustained by the Plaintiff should be reduced proportionally for the failure to mitigate such losses.

III. THIRD DEFENSE
(Illegality)

Plaintiff's claims are barred due to its own illegality and/or fraud.

IV. FORTH DEFENSE
(Unclean Hands)

Plaintiff's claims are barred, in whole or in part, by the Doctrine of Unclean Hands.

V. FIFTH DEFENSE
(Misjoinder)

There is a misjoinder of defendants. The plaintiff's Second Claim for Relief is reliant on the allegations established in paragraph 10 of the complaint. Each defendant should not be jointly or severally liable for each other and the plaintiff should respectively be barred from obtaining any relief on this basis.

VI. SIXTH DEFENSE
(No Infringement)

The piece of plaintiff's purported work allegedly copied, and represented by hash SHA1: 632613270A1D1F66429CA070C9ED5CB980357471, is not sufficiently original, fixed, or humanly perceptible to be the subject of copyright.

VII. SEVENTH DEFENSE
(Implied License)

Plaintiff claims are barred by license, express or implied.

VIII. EIGHTH DEFENSE
(Estoppel)

1 Plaintiff's claims are barred by the Doctrine of Estoppel.

2 **IX. NINTH DEFENSE**
3 (Ratification)

4 Plaintiff's claims are barred by the Doctrine of Ratification.

5 **X. TENTH DEFENSE**
6 (Barratry)

7 Plaintiff's claims are barred by barratry.

8 **XI. Eleventh**
9 (De minimis non curat lex)

10 Plaintiff's claims are barred by the equitable doctrine that the law does not concern itself with
11 trivial matters (commonly known as de minimis non curat lex).

12 **COUNTERCLAIMS**

13 As Counterclaims against Plaintiff, Defendant alleges as follows:

- 14 1. Counterclaim-plaintiff Brian Kabala has been a resident in the state of Nevada for nearly 22
15 years.
- 16 2. Counterclaim-defendant LHF Productions, Inc. is the plaintiff hereunder.
- 17 3. The Court has subject matter jurisdiction over these counterclaims under the Copyright Act,
18 the Declaratory Judgments Act, 28 U.S.C. Sections 2201-2202, and by supplemental
19 jurisdiction.
- 20 4. Venue is proper in this district because the plaintiff has consented to this district and the
21 effects of its unlawful activities are felt in this district.
- 22 5. LHF productions has filed 259 lawsuits against John Does to date. These lawsuits range
23 from March of 2016 to February of 2017 and are in multiple districts.
- 24 6. Despite Plaintiff's utilization of apparent forensic software, plaintiff has never alleged that it
25 has determined the IP address of the original source of the unique hash piece:
26 SHA1: 632613270A1D1F66429CA070C9ED5CB980357471, nor do any of the John Doe
27 cases allege that any of the John Does are the original source of the unique hash piece.
28 Plaintiff has brought no lawsuits making direct accusations against an individual or
organization of initially seeding the work into BitTorrent, creating the unique hash piece.

1 Plaintiff has brought no lawsuits against any software providers of any aspects of peer-to-
2 peer, nor against any owners or operators of websites where peer-to-peer links to *London*
3 *Has Fallen* can apparently be found. On information and belief, plaintiff has issued no
4 takedown notices under the Digital Millennium Copyright Act ("DMCA"), an act expressly
5 designed to facilitate copyright owners removing infringements of their works from the
6 internet. DMCA takedown notices are a standard part of any legitimate anti-piracy
7 campaign.

8 7. In a customary case of alleged piracy, the distribution copyright holder investigates and
9 issues take down notices to websites indexing the copyright holder's works. The websites
10 are then provided legal safe harbors for taking their subscriber's links down where there is
11 no fair use, license, or other reason to retain the link. Those links originate with seeders who
12 initially upload a work through the BitTorrent protocol to be broken into hash-valued pieces
13 indexed into a link accessible by others operating compatible protocols. Seeders/peers may
14 be fans of the work, who have a desire to comment and criticize on the work and who might
15 be fairly using and enhancing the demand for the legitimate work. The seeders/peers may
16 also be profiteers operating in violation of the law as plaintiff alleges.

17 8. Plaintiff is one of those seeders/peers operating in violation of the law.

18 9. In the Declaration of Daniel Arheidt (Dkt. No. 3, Exhibit 1 at ¶26), it is clearly stated that they
19 downloaded the entire file associated with the unique hash piece. Also in ¶26, the declarant
20 asserts that "It is possible for digital files to be mislabeled or corrupted". Because of this, the
21 file had to be downloaded every single time for each IP address to make sure it was
22 identical to *London Has Fallen*. In ¶11, it is stated: "Other users ("peers") on the network
23 connect to the seeder to download. As additional peers request the same file, each
24 additional user becomes a part of the network (or "swarm") from where the file can be
25 downloaded." In ¶12, it is stated: "This means that every "node" or peer user who has a
26 copy of the infringing copyrighted material on a P2P network can also be a source of
27 download for that infringing file, potentially both copying and distributing the infringing
28 Motion Picture."

1 10. In Dkt. No. 3, Exhibit 1 at ¶12, it is further stated: "As more peers join the swarm, the
2 likelihood of a successful download increases." This is why BitTorrent protocol makes it
3 impossible to not upload. If no peer ever uploaded, the torrent file would quickly become
4 'dead'. With respect to that, if a peer opts to not upload, that peer will quickly be unable to
5 download. See *Sean B. Karunaratne, The Case against Combating BitTorrent Piracy*
6 *through Mass John Doe Copyright Infringement Lawsuits*, 111 Mich. L. Rev. 283, 288
7 (2012). This is why the plaintiff was undoubtedly apart of the swarm that is has alleged the
8 defendants of participating in. The plaintiff consented to distributing *London Has Fallen* on a
9 P2P network because Maverickeye made them self a source for download while connected
10 to the swarm. Maverickeye did this on a continuing basis for each IP address it was
11 investigating which aided the torrent file in staying active and therefore invited more
12 "infringers" of *London Has Fallen*. If Maverickeye did not download the file for every IP
13 address, they would not be able to assess if a respective IP address was infringing and
14 would therefore make the information in 'Summary of Defendants' IP Address Data' (Dkt.
15 No. 1, Exhibit 1) baseless.

16 11. On information and belief, plaintiff is using Maverickeye UG of Germany as its "investigator."

17 12. In this case, Maverickeye UG has retained Mr. Daniel Arheidt as a consultant. For the
18 earliest lawsuits filed by the plaintiff, Maverickeye UG used Mr. Daniel Macek as a
19 consultant. Both Messrs. were retained by other anti-piracy companies before their
20 employment at Maverickeye UG. The declaration of Daniel Arheidt neglects to mention
21 Daniel Arheidt's previous experience with these other companies. In addition to the
22 declaration of Daniel Arheidt not providing his experience, it provides no education. The
23 only "qualifications" stated in the declaration are that: 1. Daniel Arheidt is competent 2. The
24 declaration is based off Daniel Arheidt's "personal knowledge" 3. Daniel Arheidt is a
25 consultant retained by Maverickeye UG.

26 13. Daniel Arheidt has also been a consultant for IPP international UG and Guardaley Ltd.
27 Guardaley has been noted for flawed and inaccurate data harvesting techniques. Guardaley
28 was a defendant in a class action lawsuit in the District of Massachusetts, Case No. 1:10-cv-

1 12043 alleging Guardaley's commission of fraud in connection with its barratrous
2 relationship with a copyright owner and law firm in bringing lawsuits based on faulty
3 investigation in order to drive nuisance settlements. Guardaley's "technology" that has been
4 used in multiple cases as plaintiffs' only evidence has also been found fundamentally flawed
5 by a German tribunal. Guardaley was sued by the German law firm Baumgarten Brandt
6 because Guardaley did not reveal the flaws in its techniques to the law firm which hired it.
7 The rulings from the German court found that Guardaley was operating a honeypot, seeding
8 its clients' own works; that Guardaley's technology identifies as infringers those who only
9 inquired about the file; that its technology identifies as infringers those who neither
10 downloaded or uploaded; and did not identify how each IP address was identified.

11 14. On information and belief, Daniel Macek provided a testimony on behalf of Maverickeye UG
12 to the Federal Court of Australia in 2015 for the *iiNet v. Dallas Buyer's Club, LLC* case.
13 During cross-examination, Daniel Macek testified that he didn't prepare his own testimony.
14 Exhibit E is a presentation by made by 'Anti-Piracy Management Company'. It's essentially
15 a template and business model for 'copyright troll' attorneys to file lawsuits against john
16 does. In page 35, it is stated, "we're hoping the judge won't question his qualifications too
17 much", in regards to Daniel Macek.

18 15. Daniel Arheidt's declaration didn't meet the requirements in Fed. R. Evid. 702 because of
19 two reasons: Firstly, part (c) was not followed, because the attorneys for the plaintiff each
20 prepared their own testimony for Daniel Arheidt to sign. Both of the declarations from Daniel
21 Macek and Daniel Arheidt were exactly same in most cases when they were submitted by
22 the same attorney; with the exception of the titles and signatures. Compare Exhibit A to
23 Exhibit B and Exhibit C to Exhibit D. The declarations are different for every district in which
24 they're filed in. Compare Exhibits A and B to Exhibits C and D. This lack of consistency and
25 Daniel Arheidt not preparing his own testimony hardly constitutes "reliable principles and
26 methods". Secondly, part (d) was not followed because Daniel Arheidt didn't prepare his
27 own testimony. He couldn't have possibly "reliably applied the principles and methods to the
28 facts of the case" because he didn't do it himself and just merely signed it. For example, the

Daniel Arheidt declaration didn't even provide the case number, yet he still signed it. This is proof Daniel Arheidt doesn't read over or prepare every declaration he signs. In ¶1 of Declaration of Daniel Arheidt, the statement, "This declaration is based on my personal knowledge", is fraudulent for the aforementioned reasons. For the reasons stated above, the Daniel Arheidt declaration didn't conform to reasoning set forth in Fed. R. Evid. 102. The plaintiff's barratrous method of mass-producing these declarations to attest to a single piece of evidence is grossly unfair to all the defendants in each case.

16. Plaintiff is operating this barratrous infringement lawsuit enterprise in Nevada with a business license, however, it doesn't have any certificates of authority to conduct business the other states in which it has filed lawsuits. On information and belief, plaintiff is paying for the "evidence" in its tables from Maverickeye UG and has agreed to share proceeds of these matters with Maverickeye UG and those responsible for creation of the tables.

17. Maverickeye UG and all of its "consultants" are not licensed private investigators in the state of Nevada or any other state. Pursuant to NRS 648.012, Maverickeye UG is clearly a private investigator. The plaintiff is in violation of NRS 648 since they elected to compensate an unlicensed private investigator for information to be used court.

COUNTERCLAIM COUNT ONE
(Declaration of non-infringement)

18. Defendant repeats all of their Answer, Affirmative Defenses, and Counterclaim as if stated here.

19. Defendant has not infringed any of plaintiff's exclusive rights in *London Has Fallen* and seeks a formal declaration of the same.

COUNTERCLAIM COUNT TWO
(Abuse of Process)

20. Defendant repeats all of their Answer, Affirmative Defenses, and Counterclaim as if stated here.

21. Plaintiff's lawsuit is an Abuse of Process. Plaintiff intends to elicit settlement funds and/or default judgements from defendants, rather than to explicitly prevent infringement of its copyrights. Moreover, Plaintiff has developed and engaged a litigation centric business

1 model, whereby Plaintiff tracks BitTorrent sites in order to locate IP addresses, which may
2 lead to a potential copyright infringer, in order to generate income off of the alleged
3 downloads rather than use this as a part of their methodology to stop infringements. The
4 Plaintiff's aforementioned actions are very similar to the processes described in pages 15 to
5 18 of Exhibit E.

6 Pursuant to FRCP 11, as amended, all possible affirmative defenses and counterclaims may
7 not have been alleged herein insofar as sufficient facts were not available after reasonable
8 inquiry upon the filing of Defendant's Answer, and therefore Defendant reserves the right to
9 amend its answer to allege additional affirmative defenses and/or counterclaims, if subsequent
10 investigation so warrants.

11 **WHEREFORE, Brian Kabala prays for:**

12 A. Dismissal of plaintiff's claims with prejudice;

13 B. An order that plaintiff shall be afforded no relief from its complaint herein;

14 C. A ruling prohibiting the testimony of Daniel Arheidt, Daniel Macek, or any
15 representative of Maverickeye UG on the basis of lack of foundation, inequitable conduct, and
16 Daubert principles;

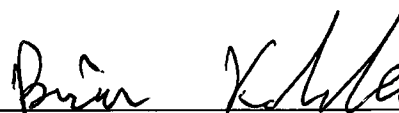
17 D. For any and all damages suffered by defendant;

18 E. Sanctions pursuant to Fed. R. Civ. P. 11; and

19 F. For such other and further relief as the Court may deem just.

20
21
22 Dated this 13th of March, 2017.

23
24 Respectfully submitted,

25 

26 Brian Kabala
27 4920 Holly Grove Drive
28 Las Vegas, Nevada 89130
Defendant Pro Se

EXHIBIT A

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON AT SEATTLE

LHF PRODUCTIONS, INC.,

Plaintiff,

v.

DOES 1-19,

Defendants.

Civil Action No. 16-cv-864

DECLARATION OF DANIEL MACEK IN
SUPPORT OF *EX PARTE* MOTION FOR
EXPEDITED DISCOVERY

I, Daniel Macek, declare as follows:

1. My name is Daniel Macek. I am over the age of 18 and am otherwise competent to make this declaration. This declaration is based on my personal knowledge and, if called upon to do so, I will testify that the facts stated herein are true and accurate.

2. I have been retained as a consultant by Maverickeye UG ("MEU"), a company incorporated in Stuttgart and organized and existing under the laws of Germany, in its technical department. MEU is in the business of providing forensic investigation services to copyright owners.

A. Peer-to-Peer Networks and the BitTorrent Protocol

3. The Internet is a vast collection of interconnected computers and computer networks that communicate with each other. It allows users to freely and easily exchange ideas

1 and information, including academic research, literary works, financial data, music, audiovisual
2 works, graphics, and an unending and ever-changing array of other data. The Internet also affords
3 opportunities for the wide-scale infringement of copyrighted motion pictures and other digital
4 content. Once a motion picture has been transformed into an unsecured digital format, it can be
5 copied further and distributed an unlimited number of times over the Internet without significant
6 degradation in picture or sound quality.

7 4. To copy and distribute copyrighted motion pictures over the Internet, many
8 individuals use online media distribution systems or so-called peer-to-peer (“P2P”) or BitTorrent
9 networks. P2P networks, at least in their most common form, are computer systems that enable
10 Internet users to (1) make files (including motion pictures) stored on each user’s computer
11 available for copying by other users; (2) search for files stored on other users’ computers; and (3)
12 transfer exact copies of files from one computer to another via the Internet.

13 5. To use a P2P or BitTorrent distribution system requires more than a click of a
14 button. A substantial software installation and computer configuration process needs to take place.
15 At any given moment and depending on the particular P2P network involved, anywhere from
16 thousands to millions of people, either across the country or around the world, unlawfully use the
17 P2P network to connect to one another’s computers to upload (distribute) or download (copy)
18 copyrighted material. The P2P systems represent a “viral” distribution or, in other words, systems
19 that enable widespread distribution of digital files: each user of the system who copies a digital
20 file from another user can then distribute the file to still other users and so on, so that complete
21 digital copies can be easily and quickly distributed thereby eliminating long download times.

22 6. Further, a person who uses a P2P network is free to use any alias (or “network
23 name”) whatsoever, without revealing his or her true identity to other users. Thus, while Plaintiff
24 has observed the infringement occurring on the Internet, it does not know the true identities of
25 those individuals who are committing the infringement.
26

1 7. Additionally, the P2P methodologies for which MEU monitored for Plaintiff's
2 motion picture make even small computers with low bandwidth capable of participating in large
3 data transfers across a P2P network. The initial file provider intentionally elects to share a file
4 using a P2P network. This is called "seeding." Other users ("peers") on the network connect to the
5 seeder to download. As additional peers request the same file, each additional user becomes a part
6 of the network (or "swarm") from where the file can be downloaded. However, unlike a traditional
7 peer-to-peer network, each new file downloader is receiving a different piece of the data from each
8 user who has already downloaded that piece of data, all of which pieces together comprise the
9 whole.

10 8. This means that every "node" or peer user who has a copy of the infringing
11 copyrighted material on a P2P network can also be a source of download for that infringing file,
12 potentially both copying and distributing the infringing work simultaneously. This distributed
13 nature of P2P leads to a rapid viral spreading of a file throughout peer users. As more peers join
14 the swarm, the likelihood of a successful download increases. Because of the nature of a P2P
15 protocol, any seed peer who has downloaded a file prior to the time a subsequent peer downloads
16 the same file is automatically a possible source for the subsequent infringement.

17 **B. Computer Forensic Identification of BitTorrent Infringement**

18 9. All infringers connected to those files are investigated through downloading a part
19 of the file placed on their computer. This evidence is then saved on a secure server. Once the
20 forensic technology identifies an infringer in the way described herein for the motion picture for
21 which Plaintiff owns the exclusive licensing and distribution rights, it automatically obtains the
22 Internet Protocol ("IP") of a user offering the file for download and saves it in a secure database.

23 10. The forensic technology used by MEU is propriety software that collects, identifies
24 and records the IP addresses in use by those people that employ the BitTorrent protocol to share,
25
26

1 copy, reproduce and distribute copyrighted works. In this way the software is connected to files of
2 illegal versions of the motion picture.

3 11. An IP address is a unique numerical identifier that is automatically assigned to an
4 Internet user by the user's Internet Service Provider ("ISP"). It only enables Plaintiff to trace the
5 infringer's access to the Internet to a particular ISP. An ISP can be a telecommunications service
6 provider such as Verizon, an Internet service provider such as America Online, a cable Internet
7 service provider such as Comcast, or even an entity such as a university that is large enough to
8 establish its own network and link directly to the Internet. Each time a subscriber logs on, he or
9 she may be assigned a different (or "dynamic") IP address unless the user obtains from his/her ISP
10 a static IP address. ISPs are assigned certain blocks or ranges of IP addresses by the Internet
11 Assigned Numbers Authority ("IANA") or a regional internet registry such as the American
12 Registry for Internet Numbers ("ARIN"). However, some ISPs lease or otherwise allocate certain
13 of their IP addresses to other unrelated, intermediary ISPs. These intermediaries can be identified
14 by the ISP and the intermediaries own logs will contain the subscriber information.

15 12. In logs kept in the ordinary course of business, ISPs keep track of the IP addresses
16 assigned to their subscribers. Once provided with an IP address, plus the date and time of the
17 detected and documented infringing activity, ISPs can use their subscriber logs to identify the
18 name, address, email address, phone number and other related information of the user/subscriber.

19 13. Only the ISP to whom a particular IP address has been assigned for use by its
20 subscribers can correlate that IP address to a particular subscriber. From time to time, a subscriber
21 of Internet services may be assigned different IP addresses from their ISP. Thus, to correlate a
22 subscriber with an IP address, the ISP also needs to know when the IP address was being used.
23 Unfortunately, many ISPs only retain for a very limited amount of time the information necessary
24 to correlate an IP address to a particular subscriber.
25
26

1 14. MEU determined that the Doe Defendants identified in Exhibit B to the complaint
2 were using the ISPs to gain access to the Internet and distribute and make available for distribution
3 and copying Plaintiff's copyrighted motion picture.

4 15. It is possible for digital files to be mislabeled or corrupted; therefore, MEU (and
5 accordingly Plaintiff) does not rely solely on the labels and metadata attached to the files
6 themselves to determine which motion picture is being unlawfully distributed. This is done through
7 a visual comparison between the version of the movie made available on file sharing networks by
8 infringers and a control copy of Plaintiff's movie. Only when it is visually confirmed that the two
9 movies are the same does monitoring for that version of the movie commence. To identify the IP
10 Addresses of those BitTorrent users who were copying and distributing Plaintiff's copyrighted
11 motion picture, MEU's forensic software scans peer-to-peer networks for the presence of
12 infringing transactions.

13 16. After reviewing the evidence logs, I isolated the transactions and the IP addresses
14 of the users responsible for copying and distributing the motion picture.

15 17. Through each of the transactions, the computers using the IP addresses identified
16 in Exhibit B to the complaint transmitted a copy or a part of a copy of a digital media file identified
17 by the hash value set forth in Exhibit B. The IP addresses, hash values, dates and times and
18 geolocation contained in Exhibit B correctly reflect what is contained in the evidence logs. The
19 subscribers using the IP addresses set forth in Exhibit B were all part of a "swarm" of users that
20 were reproducing, distributing, displaying or performing the copyrighted motion picture.

21 18. Moreover, the users were sharing the exact same copy of the motion picture. Any
22 digital copy of an audiovisual work may be uniquely identified by a unique, coded, string of
23 characters called a "hash checksum." The hash checksum is a string of alphanumeric characters
24 generated by a mathematical algorithm known as US Secure Hash Algorithm 1 or "SHA-1." Using
25
26

1 hash tag to identify different copies of the motion picture, MEU is able to confirm that these users
2 reproduced the very same copy of the motion picture.

3 19. The forensic software analyzed each BitTorrent "piece" distributed by each IP
4 address listed in Exhibit B using the SHA-1 algorithm. It verified that the piece(s) received by the
5 monitoring system form part of Plaintiff's movie.

6 20. The software uses a geolocation functionality to confirm that all IP addresses of the
7 users set forth in Exhibit B were located in the State of Washington. Though an IP address alone
8 does not reveal the name or contact information of the account holder, it does reveal the locations
9 of the Internet line used for the transaction. IP addresses are distributed to ISPs by public, nonprofit
10 organizations called Regional Internet Registries. These registries assign blocks of IP addresses to
11 ISPs by geographic region. Master tables correlating the IP addresses with local regions are
12 maintained by these organizations in a publicly available and searchable format. An IP address'
13 geographic location can be further narrowed by cross-referencing this information with secondary
14 sources such as data contributed to commercial databases by ISPs. As set forth in Exhibit B to the
15 complaint, I have confirmed not only that the users distributed the files in the State of Washington,
16 but while not always precise with respect to physical location, I list further data indicating the
17 estimated city in which the distribution took place.

18 21. Once provided with the IP address, plus the date and time of the infringing activity,
19 the Doe Defendant's ISPs quickly and easily can use their respective subscriber logs to identify
20 the name and address of the ISP subscriber who was assigned that IP address at that date and time.
21 However, ISPs typically retain user activity logs containing the information sought for only a
22 limited period of time before erasing the data.

1 I declare under penalty of perjury of the laws of the United States of America that the
2 foregoing is true and correct.

3 EXECUTED the 8 day of June, 2016.

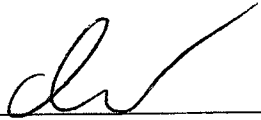
4
5 
6 Daniel Macek

EXHIBIT B

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON AT SEATTLE

LHF PRODUCTIONS, INC.,

Plaintiff,

v.

DOES 1-17,

Defendants.

Civil Action No. 16-cv-1015

DECLARATION OF DANIEL ARHEIDT
IN SUPPORT OF *EX PARTE* MOTION
FOR EXPEDITED DISCOVERY

I, Daniel Arheidt, declare as follows:

1. My name is Daniel Arheidt. I am over the age of 18 and am otherwise competent to make this declaration. This declaration is based on my personal knowledge and, if called upon to do so, I will testify that the facts stated herein are true and accurate.

2. I have been retained as a consultant by Maverickeye UG ("MEU"), a company incorporated in Stuttgart and organized and existing under the laws of Germany, in its technical department. MEU is in the business of providing forensic investigation services to copyright owners.

A. Peer-to-Peer Networks and the BitTorrent Protocol

3. The Internet is a vast collection of interconnected computers and computer networks that communicate with each other. It allows users to freely and easily exchange ideas

1 and information, including academic research, literary works, financial data, music, audiovisual
2 works, graphics, and an unending and ever-changing array of other data. The Internet also affords
3 opportunities for the wide-scale infringement of copyrighted motion pictures and other digital
4 content. Once a motion picture has been transformed into an unsecured digital format, it can be
5 copied further and distributed an unlimited number of times over the Internet without significant
6 degradation in picture or sound quality.

7 4. To copy and distribute copyrighted motion pictures over the Internet, many
8 individuals use online media distribution systems or so-called peer-to-peer (“P2P”) or BitTorrent
9 networks. P2P networks, at least in their most common form, are computer systems that enable
10 Internet users to (1) make files (including motion pictures) stored on each user’s computer
11 available for copying by other users; (2) search for files stored on other users’ computers; and (3)
12 transfer exact copies of files from one computer to another via the Internet.

13 5. To use a P2P or BitTorrent distribution system requires more than a click of a
14 button. A substantial software installation and computer configuration process needs to take place.
15 At any given moment and depending on the particular P2P network involved, anywhere from
16 thousands to millions of people, either across the country or around the world, unlawfully use the
17 P2P network to connect to one another’s computers to upload (distribute) or download (copy)
18 copyrighted material. The P2P systems represent a “viral” distribution or, in other words, systems
19 that enable widespread distribution of digital files: each user of the system who copies a digital
20 file from another user can then distribute the file to still other users and so on, so that complete
21 digital copies can be easily and quickly distributed thereby eliminating long download times.

22 6. Further, a person who uses a P2P network is free to use any alias (or “network
23 name”) whatsoever, without revealing his or her true identity to other users. Thus, while Plaintiff
24 has observed the infringement occurring on the Internet, it does not know the true identities of
25 those individuals who are committing the infringement.
26

1 7. Additionally, the P2P methodologies for which MEU monitored for Plaintiff's
2 motion picture make even small computers with low bandwidth capable of participating in large
3 data transfers across a P2P network. The initial file provider intentionally elects to share a file
4 using a P2P network. This is called "seeding." Other users ("peers") on the network connect to the
5 seeder to download. As additional peers request the same file, each additional user becomes a part
6 of the network (or "swarm") from where the file can be downloaded. However, unlike a traditional
7 peer-to-peer network, each new file downloader is receiving a different piece of the data from each
8 user who has already downloaded that piece of data, all of which pieces together comprise the
9 whole.

10 8. This means that every "node" or peer user who has a copy of the infringing
11 copyrighted material on a P2P network can also be a source of download for that infringing file,
12 potentially both copying and distributing the infringing work simultaneously. This distributed
13 nature of P2P leads to a rapid viral spreading of a file throughout peer users. As more peers join
14 the swarm, the likelihood of a successful download increases. Because of the nature of a P2P
15 protocol, any seed peer who has downloaded a file prior to the time a subsequent peer downloads
16 the same file is automatically a possible source for the subsequent infringement.

17 **B. Computer Forensic Identification of BitTorrent Infringement**

18 9. All infringers connected to those files are investigated through downloading a part
19 of the file placed on their computer. This evidence is then saved on a secure server. Once the
20 forensic technology identifies an infringer in the way described herein for the motion picture for
21 which Plaintiff owns the exclusive licensing and distribution rights, it automatically obtains the
22 Internet Protocol ("IP") of a user offering the file for download and saves it in a secure database.

23 10. The forensic technology used by MEU is propriety software that collects, identifies
24 and records the IP addresses in use by those people that employ the BitTorrent protocol to share,
25
26

1 copy, reproduce and distribute copyrighted works. In this way the software is connected to files of
2 illegal versions of the motion picture.

3 11. An IP address is a unique numerical identifier that is automatically assigned to an
4 Internet user by the user's Internet Service Provider ("ISP"). It only enables Plaintiff to trace the
5 infringer's access to the Internet to a particular ISP. An ISP can be a telecommunications service
6 provider such as Verizon, an Internet service provider such as America Online, a cable Internet
7 service provider such as Comcast, or even an entity such as a university that is large enough to
8 establish its own network and link directly to the Internet. Each time a subscriber logs on, he or
9 she may be assigned a different (or "dynamic") IP address unless the user obtains from his/her ISP
10 a static IP address. ISPs are assigned certain blocks or ranges of IP addresses by the Internet
11 Assigned Numbers Authority ("IANA") or a regional internet registry such as the American
12 Registry for Internet Numbers ("ARIN"). However, some ISPs lease or otherwise allocate certain
13 of their IP addresses to other unrelated, intermediary ISPs. These intermediaries can be identified
14 by the ISP and the intermediaries own logs will contain the subscriber information.

15 12. In logs kept in the ordinary course of business, ISPs keep track of the IP addresses
16 assigned to their subscribers. Once provided with an IP address, plus the date and time of the
17 detected and documented infringing activity, ISPs can use their subscriber logs to identify the
18 name, address, email address, phone number and other related information of the user/subscriber.

19 13. Only the ISP to whom a particular IP address has been assigned for use by its
20 subscribers can correlate that IP address to a particular subscriber. From time to time, a subscriber
21 of Internet services may be assigned different IP addresses from their ISP. Thus, to correlate a
22 subscriber with an IP address, the ISP also needs to know when the IP address was being used.
23 Unfortunately, many ISPs only retain for a very limited amount of time the information necessary
24 to correlate an IP address to a particular subscriber.

1 14. MEU determined that the Doe Defendants identified in Exhibit B to the complaint
2 were using the ISPs to gain access to the Internet and distribute and make available for distribution
3 and copying Plaintiff's copyrighted motion picture.

4 15. It is possible for digital files to be mislabeled or corrupted; therefore, MEU (and
5 accordingly Plaintiff) does not rely solely on the labels and metadata attached to the files
6 themselves to determine which motion picture is being unlawfully distributed. This is done through
7 a visual comparison between the version of the movie made available on file sharing networks by
8 infringers and a control copy of Plaintiff's movie. Only when it is visually confirmed that the two
9 movies are the same does monitoring for that version of the movie commence. To identify the IP
10 Addresses of those BitTorrent users who were copying and distributing Plaintiff's copyrighted
11 motion picture, MEU's forensic software scans peer-to-peer networks for the presence of
12 infringing transactions.

13 16. After reviewing the evidence logs, I isolated the transactions and the IP addresses
14 of the users responsible for copying and distributing the motion picture.

15 17. Through each of the transactions, the computers using the IP addresses identified
16 in Exhibit B to the complaint transmitted a copy or a part of a copy of a digital media file identified
17 by the hash value set forth in Exhibit B. The IP addresses, hash values, dates and times and
18 geolocation contained in Exhibit B correctly reflect what is contained in the evidence logs. The
19 subscribers using the IP addresses set forth in Exhibit B were all part of a "swarm" of users that
20 were reproducing, distributing, displaying or performing the copyrighted motion picture.

21 18. Moreover, the users were sharing the exact same copy of the motion picture. Any
22 digital copy of an audiovisual work may be uniquely identified by a unique, coded, string of
23 characters called a "hash checksum." The hash checksum is a string of alphanumeric characters
24 generated by a mathematical algorithm known as US Secure Hash Algorithm 1 or "SHA-1." Using
25
26

1 hash tag to identify different copies of the motion picture, MEU is able to confirm that these users
2 reproduced the very same copy of the motion picture.

3 19. The forensic software analyzed each BitTorrent “piece” distributed by each IP
4 address listed in Exhibit B using the SHA-1 algorithm. It verified that the piece(s) received by the
5 monitoring system form part of Plaintiff’s movie.

6 20. The software uses a geolocation functionality to confirm that all IP addresses of the
7 users set forth in Exhibit B were located in the State of Washington. Though an IP address alone
8 does not reveal the name or contact information of the account holder, it does reveal the locations
9 of the Internet line used for the transaction. IP addresses are distributed to ISPs by public, nonprofit
10 organizations called Regional Internet Registries. These registries assign blocks of IP addresses to
11 ISPs by geographic region. Master tables correlating the IP addresses with local regions are
12 maintained by these organizations in a publicly available and searchable format. An IP address’
13 geographic location can be further narrowed by cross-referencing this information with secondary
14 sources such as data contributed to commercial databases by ISPs. As set forth in Exhibit B to the
15 complaint, I have confirmed not only that the users distributed the files in the State of Washington,
16 but while not always precise with respect to physical location, I list further data indicating the
17 estimated city in which the distribution took place.

18 21. Once provided with the IP address, plus the date and time of the infringing activity,
19 the Doe Defendant’s ISPs quickly and easily can use their respective subscriber logs to identify
20 the name and address of the ISP subscriber who was assigned that IP address at that date and time.
21 However, ISPs typically retain user activity logs containing the information sought for only a
22 limited period of time before erasing the data.

1 I declare under penalty of perjury of the laws of the United States of America that the
2 foregoing is true and correct.

3 EXECUTED the 30 day of June, 2016.

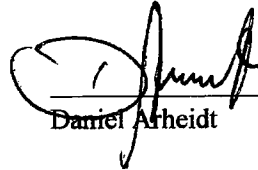
4
5 
6 Daniel Arheidt
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26

EXHIBIT C

Judge Samuel Der-Yeghiayan

1. My name is Daniel Macek. I am over the age of 18 and am otherwise competent to make this declaration. This declaration is based on my personal knowledge and, if called upon to do so, I will testify that the facts stated herein are true and accurate.
2. I have been retained as a consultant by Maverickeye UG ("MEU"), a company incorporated in Stuttgart and organized and existing under the laws of Germany, in its technical department. MEU is in the business of providing forensic investigation services to copyright owners.
3. The Internet is a vast collection of interconnected computers and computer networks that communicate with each other. It allows users to freely and easily exchange ideas and information, including academic research, literary works, financial data, music, audiovisual works, graphics, and an unending and ever-changing array of other data.
4. The Internet also affords opportunities for the wide-scale infringement of copyrighted motion pictures and other digital content.
5. Once a motion picture has been transformed into a digital format, it can be copied further and distributed an unlimited number of times over the Internet, without significant degradation in picture or sound quality.
6. To copy and distribute copyrighted motion pictures over the Internet, many individuals use online media distribution systems or so-called peer-to-peer ("P2P") or BitTorrent networks. P2P networks,

16-cv-4744

at least in their most common form, are computer systems that enable Internet users to (1) make files (including motion pictures) stored on each user's computer available for copying by other users; (2) search for files stored on other users' computers; and (3) transfer exact copies of files from one computer to another via the Internet.

7. To use a P2P or BitTorrent distribution system requires more than a click of a button. A software installation and configuration process needs to take place.

8. The P2P systems enable widespread distribution of digital files: each user of the system who copies a digital file from another user can then distribute the file to other users and so on, so that complete digital copies can be easily and quickly distributed thereby eliminating long download times.

9. While Plaintiff has observed the infringement occurring on the Internet, it does not know the true identities of those individuals who are committing the infringement.

10. Additionally, the P2P methodologies which Maverickeye UG monitored for Plaintiff's Motion Picture (*London Has Fallen*) make even small computers with low bandwidth capable of participating in large data transfers across a P2P network. The initial file-provider intentionally elects to share a file using a P2P network. This is called "seeding." Other users ("peers") on the network connect to the seeder to download. As additional peers request the same file, each additional user becomes a part of the network (or "swarm") from which the file can be downloaded. However, unlike a traditional peer-to-peer network, each new file downloader is receiving a different piece of the data from each user who has already downloaded that piece of data, all of which pieces together comprise the whole.

11. This means that every "node" or peer user who has a copy of the infringing copyrighted material on a P2P network can also be a source of download for that infringing file, potentially both copying and distributing the copyrighted Motion Picture. The distributed nature of P2P leads to rapid spreading of a file throughout peer users. As more peers join the swarm, the likelihood of a successful download increases. Because of the nature of a P2P protocol, any seed peer who has downloaded a file prior to the time a subsequent peer downloads the same file is automatically a possible source for the subsequent peer.

16-cv-4744

12. All infringers connected to those files are investigated through downloading a part of the file placed on their computer.

13. This evidence is then saved on a secure server.

14. Once the searching software program identifies an infringer in the way described herein for the Motion Picture for which Plaintiff owns the exclusive licensing and distribution rights, it automatically obtains the IP address of a user offering the file for download and saves it in a secure database.

15. The forensic software routinely collects, identifies and records the Internet Protocol ("IP") addresses in use by those people who employ the BitTorrent protocol to share, copy, reproduce and distribute copyrighted works. In this way, the software is connected to files of illegal versions of the Motion Picture.

16. An IP address is a unique numerical identifier that is automatically assigned to an Internet user by the user's Internet Service Provider ("ISP"). It only enables Plaintiff to trace the infringer's access to the Internet to a particular ISP. An ISP can be a telecommunications service provider such as Verizon, an Internet service provider such as America Online, a cable Internet service provider such as Comcast, or even an entity such as a university that is large enough to establish its own network and link directly to the Internet. Each time a subscriber logs on, he or she may be assigned a different (or "dynamic") IP address unless the user obtains from his/her ISP a static IP address. ISPs are assigned certain blocks or ranges of IP addresses by the Internet Assigned Numbers Authority ("IANA") or a regional internet registry such as the American Registry for Internet Numbers ("ARIN"). However, some ISPs lease or otherwise allocate certain of their IP addresses to other unrelated, intermediary ISPs. These intermediaries can be identified by the ISP, and the logs of the intermediaries will contain the subscriber information.

17. In logs kept in the ordinary course of business, ISPs keep track of the IP addresses assigned to their subscribers. Once provided with an IP address, plus the date and time of the detected and documented infringing activity, ISPs can use their subscriber logs to identify the name, address, email address, phone number and other related information of the user/subscriber.

16-cv-4744

18. Only the ISP to whom a particular IP address has been assigned for use by its subscribers can correlate that IP address to a particular subscriber. From time to time, a subscriber of Internet services may be assigned different IP addresses from their ISP. Thus, to correlate a subscriber with an IP address, the ISP also needs to know when the IP address was being used.

19. Maverickeye UG determined that the Doe Defendants identified in Complaint Exhibit B were using the ISPs listed in the exhibit to gain access to the Internet and distribute and make available for distribution and copying Plaintiff's copyrighted Motion Picture.

20. It is possible for digital files to be mislabeled or corrupted; therefore, Maverickeye UG (and accordingly, Plaintiff) does not rely solely on the labels and metadata attached to the files themselves to determine whether or not a particular motion picture is copied in the downloaded file, but also confirms the copying by a visual comparison of the downloaded file and the Motion Picture.

21. As to Plaintiff's copyrighted Motion Picture, as identified in the Complaint, a member of Maverickeye UG watches a DVD of the original Motion Picture.

22. After Maverickeye UG identifies the Doe Defendants and downloads the motion pictures they were distributing, Maverickeye UG opens the downloaded files, watches them and confirms that they contain the Motion Picture identified in the Complaint.

23. To identify the IP addresses of those BitTorrent users who were copying and distributing Plaintiff's copyrighted Motion, Maverickeye UG's forensic software scans peer-to-peer networks for the presence of infringing transactions.

24. After reviewing the evidence logs, I isolated the transactions and the IP addresses of the users responsible for copying and distributing the Motion Picture.

25. Through each of the transactions, the computers using the IP addresses identified in Complaint Exhibit B transmitted a copy or a part of a copy of a digital media file of the copyrighted Motion Picture identified by the hash value set forth in Complaint Exhibit B. The IP addresses, hash values, dates and times contained in Complaint Exhibit B correctly reflect what is contained in the evidence logs. The subscribers using the IP addresses set forth in Complaint Exhibit B were all part of a single "swarm" of

16-cv-4744

users who were reproducing, distributing, displaying or performing the copyrighted Motion Picture on April 13, 2016.

26. Moreover, the users were sharing the exact same copy of the Motion Picture. Any digital copy of an audiovisual work may be uniquely identified by a unique, coded, string of characters called a "hash checksum." The hash checksum is a string of alphanumeric characters generated by a mathematical algorithm known as US Secure Hash Algorithm 1 or "SHA-1." By using a hash tag to identify different copies of the Motion Picture, MEU was able to confirm that these users reproduced the very same copy of the Motion Picture.

27. The MEU software analyzed each BitTorrent "piece" distributed by each IP address listed in Complaint Exhibit B and verified that reassembling the pieces using a specialized BitTorrent client results in a fully playable digital motion picture.

28. The software uses a geolocation functionality to determine the location of the IP addresses under investigation. The location of each IP address is set forth in Complaint Exhibit B. IP addresses are distributed to ISPs by public, nonprofit organizations called Regional Internet Registries. These registries assign blocks of IP addresses to ISPs by geographic region. Master tables correlating the IP addresses with local regions are maintained by these organizations in a publicly-available and searchable format. An IP address' geographic location can be further narrowed by cross-referencing this information with secondary sources such as data contributed to commercial database by ISPs.

29. I acknowledge that there were other swarms, employing different "seed files," through which others copied and distributed Plaintiff's copyrighted Motion Picture before, during and after the timeframe referenced in Paragraph 25 above. Plaintiff, however, has limited the pool of Defendants in this lawsuit only to those who downloaded the movie from a single seed file in a brief and definite temporal period, specifically with the intent to prosecute an action only against defendants who were involved in the same transaction, occurrence, or series of transactions or occurrences.

16-cv-4744

PURSUANT TO 28 U.S.C. § 1746, I hereby declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on this 12 day of May 2016.

By: 
Daniel Macek

EXHIBIT D

)
)
) **Case No.: 16-cv-6797**
)
)
) **Judge Samuel Der-Yeghiayan**
)
)
)

6. To copy and distribute copyrighted motion pictures over the Internet, many individuals use online media distribution systems or so-called peer-to-peer ("P2P") or BitTorrent networks. P2P networks,

16-cv-6797

at least in their most common form, are computer systems that enable Internet users to (1) make files (including motion pictures) stored on each user's computer available for copying by other users; (2) search for files stored on other users' computers; and (3) transfer exact copies of files from one computer to another via the Internet.

7. To use a P2P or BitTorrent distribution system requires more than a click of a button. A software installation and configuration process needs to take place.

8. The P2P systems enable widespread distribution of digital files: each user of the system who copies a digital file from another user can then distribute the file to other users and so on, so that complete digital copies can be easily and quickly distributed thereby eliminating long download times.

9. While Plaintiff has observed the infringement occurring on the Internet, it does not know the true identities of those individuals who are committing the infringement.

10. Additionally, the P2P methodologies which Maverickeye UG monitored for Plaintiff's Motion Picture (*London Has Fallen*) make even small computers with low bandwidth capable of participating in large data transfers across a P2P network. The initial file-provider intentionally elects to share a file using a P2P network. This is called "seeding." Other users ("peers") on the network connect to the seeder to download. As additional peers request the same file, each additional user becomes a part of the network (or "swarm") from which the file can be downloaded. However, unlike a traditional peer-to-peer network, each new file downloader is receiving a different piece of the data from each user who has already downloaded that piece of data, all of which pieces together comprise the whole.

11. This means that every "node" or peer user who has a copy of the infringing copyrighted material on a P2P network can also be a source of download for that infringing file, potentially both copying and distributing the copyrighted Motion Picture. The distributed nature of P2P leads to rapid spreading of a file throughout peer users. As more peers join the swarm, the likelihood of a successful download increases. Because of the nature of a P2P protocol, any seed peer who has downloaded a file prior to the time a subsequent peer downloads the same file is automatically a possible source for the subsequent peer.

16-cv-6797

12. All infringers connected to those files are investigated through downloading a part of the file placed on their computer.

13. This evidence is then saved on a secure server.

14. Once the searching software program identifies an infringer in the way described herein for the Motion Picture for which Plaintiff owns the exclusive licensing and distribution rights, it automatically obtains the IP address of a user offering the file for download and saves it in a secure database.

15. The forensic software routinely collects, identifies and records the Internet Protocol ("IP") addresses in use by those people who employ the BitTorrent protocol to share, copy, reproduce and distribute copyrighted works. In this way, the software is connected to files of illegal versions of the Motion Picture.

16. An IP address is a unique numerical identifier that is automatically assigned to an Internet user by the user's Internet Service Provider ("ISP"). It only enables Plaintiff to trace the infringer's access to the Internet to a particular ISP. An ISP can be a telecommunications service provider such as Verizon, an Internet service provider such as America Online, a cable Internet service provider such as Comcast, or even an entity such as a university that is large enough to establish its own network and link directly to the Internet. Each time a subscriber logs on, he or she may be assigned a different (or "dynamic") IP address unless the user obtains from his/her ISP a static IP address. ISPs are assigned certain blocks or ranges of IP addresses by the Internet Assigned Numbers Authority ("IANA") or a regional internet registry such as the American Registry for Internet Numbers ("ARIN"). However, some ISPs lease or otherwise allocate certain of their IP addresses to other unrelated, intermediary ISPs. These intermediaries can be identified by the ISP, and the logs of the intermediaries will contain the subscriber information.

17. In logs kept in the ordinary course of business, ISPs keep track of the IP addresses assigned to their subscribers. Once provided with an IP address, plus the date and time of the detected and documented infringing activity, ISPs can use their subscriber logs to identify the name, address, email address, phone number and other related information of the user/subscriber.

16-cv-6797

18. Only the ISP to whom a particular IP address has been assigned for use by its subscribers can correlate that IP address to a particular subscriber. From time to time, a subscriber of Internet services may be assigned different IP addresses from their ISP. Thus, to correlate a subscriber with an IP address, the ISP also needs to know when the IP address was being used.

19. Maverickeye UG determined that the Doe Defendants identified in Complaint Exhibit B were using the ISPs listed in the exhibit to gain access to the Internet and distribute and make available for distribution and copying Plaintiff's copyrighted Motion Picture.

20. It is possible for digital files to be mislabeled or corrupted; therefore, Maverickeye UG (and accordingly, Plaintiff) does not rely solely on the labels and metadata attached to the files themselves to determine whether or not a particular motion picture is copied in the downloaded file, but also confirms the copying by a visual comparison of the downloaded file and the Motion Picture.

21. As to Plaintiff's copyrighted Motion Picture, as identified in the Complaint, a member of Maverickeye UG watches a DVD of the original Motion Picture.

22. After Maverickeye UG identifies the Doe Defendants and downloads the motion pictures they were distributing, Maverickeye UG opens the downloaded files, watches them and confirms that they contain the Motion Picture identified in the Complaint.

23. To identify the IP addresses of those BitTorrent users who were copying and distributing Plaintiff's copyrighted Motion, Maverickeye UG's forensic software scans peer-to-peer networks for the presence of infringing transactions.

24. After reviewing the evidence logs, I isolated the transactions and the IP addresses of the users responsible for copying and distributing the Motion Picture.

25. Through each of the transactions, the computers using the IP addresses identified in Complaint Exhibit B transmitted a copy or a part of a copy of a digital media file of the copyrighted Motion Picture identified by the hash value set forth in Complaint Exhibit B. The IP addresses, hash values, dates and times contained in Complaint Exhibit B correctly reflect what is contained in the evidence logs. The subscribers using the IP addresses set forth in Complaint Exhibit B were all part of a single "swarm" of

16-cv-6797

users who were reproducing, distributing, displaying or performing the copyrighted Motion Picture on April 17, 2016.

26. Moreover, the users were sharing the exact same copy of the Motion Picture. Any digital copy of an audiovisual work may be uniquely identified by a unique, coded, string of characters called a "hash checksum." The hash checksum is a string of alphanumeric characters generated by a mathematical algorithm known as US Secure Hash Algorithm 1 or "SHA-1." By using a hash tag to identify different copies of the Motion Picture, MEU was able to confirm that these users reproduced the very same copy of the Motion Picture.

27. The MEU software analyzed each BitTorrent "piece" distributed by each IP address listed in Complaint Exhibit B and verified that reassembling the pieces using a specialized BitTorrent client results in a fully playable digital motion picture.

28. The software uses a geolocation functionality to determine the location of the IP addresses under investigation. The location of each IP address is set forth in Complaint Exhibit B. IP addresses are distributed to ISPs by public, nonprofit organizations called Regional Internet Registries. These registries assign blocks of IP addresses to ISPs by geographic region. Master tables correlating the IP addresses with local regions are maintained by these organizations in a publicly-available and searchable format. An IP address' geographic location can be further narrowed by cross-referencing this information with secondary sources such as data contributed to commercial database by ISPs.

29. I acknowledge that there were other swarms, employing different "seed files," through which others copied and distributed Plaintiff's copyrighted Motion Picture before, during and after the timeframe referenced in Paragraph 25 above. Plaintiff, however, has limited the pool of Defendants in this lawsuit only to those who downloaded the movie from a single seed file in a brief and definite temporal period, specifically with the intent to prosecute an action only against defendants who were involved in the same transaction, occurrence, or series of transactions or occurrences.

16-cv-6797

PURSUANT TO 28 U.S.C. § 1746, I hereby declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on this 15 day of July 2016.

By: 
Daniel Arheidt

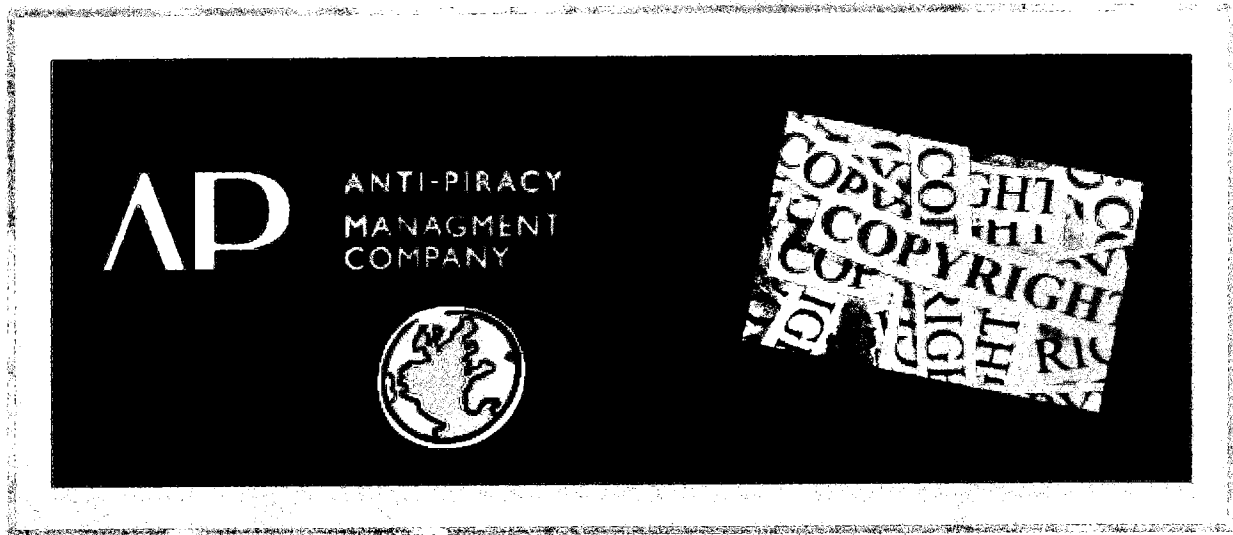
EXHIBIT E

Anti-Piracy Management Company

What is APMC?.....	4
What Services Do APMC Provide?	4
WHAT IS THE PURPOSE OF THE CEBU OFFICE?.....	4
APMC.....	4
CLIENTS	5
LAWYERS	5
INFRINGEMENTS.....	5
COURT	5
Case Management System (CMS)	5
Where is APMC's Core Business	5
What is the Legal Process in the U.S.?	5
What is APMC's problem of the U.S. legal system?	5
How do we maintain a coherent litigation strategy to issue a claim?	5
Is APMC the good guys or the bad guys?	5
How will APMC deal & counter with the opponent lawyers?	6
What is APMC's ultimate goal toward the infringers?	6
What is APMC's end result?	6
What is BPO Cebu Office's Core Business?	6
HOW DO WE FIND THE INFRINGEMENTS?	6
Structures of APMC.....	8
SALES TEAM	8
Marketing.....	8
Reporting	9
Lead Generation.....	10
Chain of Delivery/Chain of Rights	10
Contract	11
CRM (Podio)	12
Title Allocation Report (TAR Analysis).....	13
Services	14

Newsletters	14
What are the tasks of the Document Production Admin Team?	14
Task 1:	14
Task 2:	14
Task 3:	15
Task 4:	15
Task 5:	15
Task 6:	15
Task 7:	15
Task 8:	15
Task 9:	15
Steps for starting a case (Stage 1)	15
Step 1	15
Step 2	15
Step 3	16
Step 4	16
Step 5	16
Step 6	16
Step 7	16
Steps for starting a case (Stage 2)	17
Step 1	17
Step 2	17
Step 3	17
What are the essential functions of the Case Management System (CMS) development team?	18
What kind of copyrights does APMC focus on?	18
What are the functions of the LEGAL team?	19
How Do We Start a Lawsuit in the US?	19
What are statutory damages?	19
Podio	20
1. Basic Information of Podio	20
2. Podio Introduction Video	20
3. Podio Task Tutorial	20

4. PODIO (How Work APPS are Built)?	21
5. PODIO Filter Tutorial	21
6. Podio (How to Store Documents Tutorial)	21
7. Other Podio Tutorials (See YouTube videos)	22
How Can Podio Be Used to Track Copyright Documents?	22
1. Client Chain of Title	22
2. Client Copyright Registration Certificate	23
3. Anti-piracy Contract (i.e., who has the rights, the territory, terms, etc.)	23
4. Corporate Disclosure Statement - What's the meaning of this document?	23
What's the reason of a Corporate Disclosure Statement?	23
Overview on Podio Training	23
Podio Information for CRM Tool	24
Other Important Podio APPS	26
YouTube Anti-Piracy Procedures	28
Part 1: Reporting to YouTube Copyright Infringement	28
Part II: Counter Notices	28
What is a Complaint or How do you file a lawsuit in the US?	30
What are the relevant things to note on completing the 1st Document, or the complaint letter? (i.e., when editing a complaint letter)	30
The 1st Section is called the Complaint (Reference from Training Documents File: Complaint 081112)	31
The 2nd Section is called the Jurisdiction & Venue	31
The 3rd Section is called the Joiner	31
The 4th Section is called the Parties	32
The 5th Section is called the Statement of Facts	33
The 6th Section is called the Direct Copyright Infringement (Count 1) (i.e., the infringement of an "exclusive" right)	34
What's the difference between actual & statutory damages?	35



What is APMC?

It's a company providing copyright monitor protection for clients.

What Services Do APMC Provide?

APMC offers full service, expedited copyrighting of your intellectual properties when there are judicial requirements.

Our proven technology can track, identify, and match copyright infringers to real people. APMC will not hesitate to negotiate pre-court settlements or file a lawsuit against internet infringers.

APMC will give you the peace of mind you need today and tomorrow, in professionally protecting your copyright material.

WHAT IS THE PURPOSE OF THE CEBU OFFICE?

1. Make the lawyers' lives easier.
2. To assist with the client managements outsourcing
3. Handle the data extraction process.

APMC

APMC stays in the background where they are invisible, but we are the center (i.e., "we make things happen").

CLIENTS

1. We bring the clients to the law firms.
2. We managed their legal strategy.

LAWYERS

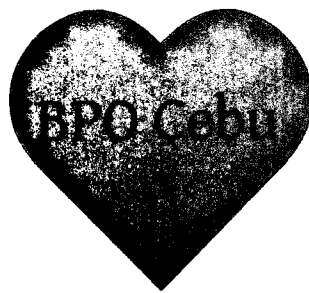
1. Law firms deal with the infringers.
2. The Lawyers' go to the court to obtain court orders in order to get disclosure of names and addresses from the internet providers.

INFRINGERS

People illegally using software and distributing without the clients permission.

COURT

1. The courts will issue a subpoena for the infringers IP names and addresses.



Case Management System (CMS)

1. The purpose is to assist the law firms with their cases.

Where is APMC's Core Business

APMC's core business is the U.S. (i.e., very sophisticated clients)

What is the Legal Process in the U.S.?

Each state has it's own legal system, so a lawyer in one state cannot issue proceedings in another state.

What is APMC's problem of the U.S. legal system?

The end result is that APMC had to recruit many lawyers, which is too expensive.

How do we maintain a coherent litigation strategy to issue a claim?

You cannot do it without a substantial team behind you.

Is APMC the good guys or the bad guys?

For APMC's clients, lawyers, & courts, we are the good guys.

APMC believes that we are the "good guys," because we're contributing to the economy (i.e., protecting jobs for producers, directors, sales agents, distribution, etc.)

For the infringers, modern day hippies, opponent lawyers, Bit Torrent, Isohunt, Pirate Bay, etc., we are the bad guys.

How will APMC deal & counter with the opponent lawyers?

APMC will create a Public Relations (PR) Cebu Team to create counter letters & other positive public relation advertisements to promote APMC's claim that we're contributing to the economy.

What is APMC's ultimate goal toward the infringers?

To clam down on the infringers to stop them of what their doing!!!

What is APMC's end result?

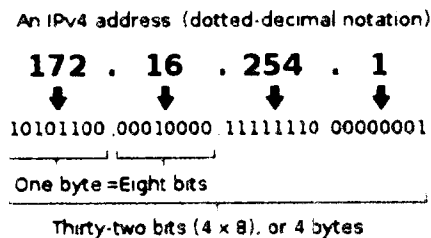
To spread the judgments far & wide in order to convince the courts (i.e. judges) that APMC is doing the right thing!

What is BPO Cebu Office's Core Business?

1. The BPO Cebu Office will make our outsourcing program a lot more attractive for lawyers, because we'll be doing a lot of the work for them.
2. The BPO Cebu Office doesn't actually require highly skilled lawyers, to do a lot of the work.
3. The BPO Cebu Office will be doing all of the document production for the lawyers.

HOW DO WE FIND THE INFRINGERS?

Internet Protocol (IP): The system of communication standards that ensures that data packets transmitted over the internet reach their intended destinations.



IP Address: The unique identifying number of a device connected to the internet.

Uniform Resource Locator (URL): The internet address assigned to a web document or resource by which it can be accessed by all web browsers.

Example:



File: A collection of related data packets treated as unit.

Hash Identifier: A 40 character alphanumeric string that forms a unique identifier of an encoded file.

Hypertext Transfer Protocol (HTTP): A system of communication standards that websites use to communicate with web browsers.

BitTorrent: A peer-to-peer file sharing protocol.

Swarm: A group of peers sharing a particular file (identified by its unique hash identifier). A swarm has two types of peers -- "leechers" and "seeds". It bears reiterating: to constitute a swarm all of the peers must be sharing the same file (identified by its unique hash identifier).

Peer: A BitTorrent user.

Initial Seeder: A BitTorrent user who first takes a particular file (such as a movie), breaks it into pieces, encodes the pieces with hash identifiers, creates a torrent file with the data about that file and its tracker, and makes the complete file available to other BitTorrent users.

Seed: A peer who downloaded a complete file and is uploading all of its pieces to other peers in the swarm.

Leecher: A peer in the process of downloading the file from the other peers. As soon as a leecher downloads new content (a piece of the file), the leecher begins sharing its content with the other leechers in the swarm.

Piece: A one-quarter megabyte size part of a file being shared via BitTorrent (except for the last, smaller piece which is the size of the remainder of the file).

Tracker: A server containing an updated list of peers in swarm. It allows a peer to learn about other peers sharing a particular torrent and join the swarm.

Torrent file: The hub of the BitTorrent system, a torrent file is a small file containing the file name, the IP address of the tracker, the number of and size of the pieces, and the hash identifier unique to the pieces of that particular torrent file.

BitTorrent index server: A server containing a list of .torrent files. Essentially a menu of available files, the BitTorrent index server is different from a tracker, which coordinated communication between peers seeking to download the content that the .torrent file describes.

Structures of APMC

SALES TEAM

How do we get a movie client?

* When a movie gets pirated, then APMC contacts the client to protect their copyrights by litigating the infringers.

Marketing

3 Ways to Approach a New Client

1. 1 If client has been pirated.
2. 2 Advertising (i.e., usabit.com or imdb.com)
3. 3 Film Festival

Film Festivals

What is APMC's Marketing 3rd Approach of Getting New Clients?

What are the 5 Steps in Preparing for Film Festivals?

1. The Sales Team gets an exhibitor's list of 100 companies attending the film festival market.

The sales team has to identify the potential clients they want to meet.

Some clients won't be suitable for APMC based on company profile, territory, etc.

The BPO Sales Team will learn based on experience which film festival clients would be the best suitable for APMC.

2. Look for a potential clients based on APMC's territories (i.e., UK, Germany, Scandinavia, US, Canada, Australia, & Japan).

The Sales Team should not select potential clients in territories that APMC don't do, such as Russia, Brazil, China, Spain, Mexico, etc.

3. Obtain the name of APMC's preferred client

Get the name in the preferred company (i.e., CEO, Managing Director, or Legal Advisor).
Create an Excel spreadsheet for potential clients with names, addresses, phone numbers, schedule availability, etc.

For existing clients, APMC already has the contact names, addresses, phone numbers, etc., so we don't have to input on Excel spreadsheet.

4. Sent our emails to APMC's preferred client telling them:

The purpose of the email is to request for a meeting and to discuss APMC's program.

For APMC, send personalize emails to potential clients, so that they know about APMC anti-piracy assistance.

Telling them Patrick & Dan from APMC will attend the film festival.

Telling them if they would like to meet.

Confirm the phone number (i.e., cellphone)

Use email tools, such as group mail, or mail chimp to sent out massive emails at one time.

Using group email (2-3 weeks before the film festival).

Wait for the Email Replies

Usually follow-up within 7-14 days.

If no reply, say, "We still haven't gotten a reply?"

If we're getting in replies, then create a schedule for Patrick & Dan.

5. Create a schedule for APMC's sales agents giving 100% accurate information of the following:

1. The name of company, film, or production company.
2. The name of the person representing the potential client.
3. The person's contact phone number (i.e., it's best to use the cell phone number due to different time zones).
4. the time of the scheduled meeting (i.e., date & time).
5. the location to meet (i.e., the hotel's conference room name & room number).

Note: to save time, use the old film festival template & just update the new client information.

Reporting

Sales Team task to find a pirated client:

- www.usabit.com (i.e. how APMC finds pirated movies websites)
- www.imdb.com (i.e. to find the rights holder)
- www.isohunt.com (APMC pursues if the "seeders" are more than 100 seeds and a High Profile Client)

APMC is focusing on high-profile clients (i.e., who are wealthy & likely to settle).

Use Abocabo and Podio to complete the reporting process.

Sales Frequently Asked Questions (FAQ)

If a client asks you a specific question, the BPO Cebu Office can give them a consistent reply (i.e., the answers will be the same for all BPO Cebu staff)

BPO Cebu Office will use Podio's Sales Q & A APP.

Purpose: Consistent replies & consistent FAQ's when communicating with potential clients.

Lead Generation

APMC's 3-Step Approach

1. Using www.usabit.com to research the following:

- Search for movie clients no earlier than the year 2000.
- Scan about 5 pages & make notes of the client.

2. Search for movie client information on www.imdb.com (i.e. detail information on producer names, addresses, contact numbers, and email addresses)

3. Obtain the name of APMC's preferred client (i.e., CEO, Managing Director, or Legal Advisor).

4. Sent our emails to APMC's preferred client using group email (2-3 weeks before the film festival).

5. Create a schedule for APMC's sales agents giving 100% accurate information of (contact name, contact cell phone #, time of meeting, and location).

2. Look for a potential client based on APMC's territories (i.e., UK, Germany, Scandanavia, US, Canada, Australia, & Japan).

Chain of Delivery/Chain of Rights

3 Types of Clients

1. Production Client (i.e., they create the movie so they own the copyrights.). If they're too busy, then hire Sales Agents.

2. Sales Agents Clients (i.e., will use 1-3 more production companies to advertise their catalog of movie clients).

3. Distributor's client (i.e., the sales agents will sell the movie to distributors' of other countries).

Who in this chain of rights is suffering from piracy?

Usually, the production company & sales agents work closely together for efficient distribution of their movies.

If a sales agent sell the rights of a movie to a distribution company that's not our client and the production company is not our client, then APMC cannot enforce those rights.

If the sales agent is able to persuade the production company or the distribution to join APMC, then APMC can do business, because the copyright are in APMC control.

Possible gray area (i.e., if a sales agent says, "We have that right," APMC doesn't pursue because of huge fights in the courts of assertion of rights).

APMC focuses on rights of a production & distribution company to go for the copyright itself.

Contract

APMC requires the following 3 documents to begin process with a new client:

1. Corporate Disclosure Statement.
2. Anti-Piracy Service Agreement.
3. Motion Certificate or Copyright Registration Certificate.

Contracts that don't need amending go straight to PA or Dan for signing.

Contracts that need amending, need changed text (i.e., Word Doc Track Changes) for PA or Dan can quickly scan, approve, & sign.

Data Gathering (Coordinated between the Sales & Document Production Admin Teams)

Store the data in the client relation management (CRM).

It's important to know exactly who is the actual client is??? (i.e., the Conjuring's producers, sales agents, or distributors)

How do you send data gathering information to a law firm?

The Sales team involves the Document Production Admin Team who has to read it, revise it, using Book marks, to make sure everything is correct.

Next, we organize all the data information into a neat packet and send to the lawyers/law firms.

Then, we store all the data gathering information into our own management system (i.e. Abocado)

To check how our asset is doing, we can use public data bases (i.e., rfcexpress.com or pacer.com) to confirm how our asset is proceeding in the courts.

Also, after 7-14 days, if no email reply from the lawyer/law firm, then we contact them to check the status of our asset. (i.e., by phone or reminder letter).

Eventually, the lawyer corresponds to APMC that the court has responded with our documents (i.e., subpoenas).

Then, the lawyers get the ISP names & addresses & compiles it into paper data (i.e., spreadsheets).

APMC collects this information & puts it into our CMS.

Next, APMC generates the letter & gives it back to the lawyer to double check the quality standard of the document & sends out the letter to the infringer(s).

In real time, when the lawyer sends out the letter, its the start of the delivery of an asset.

BPO Cebu Office will assist the lawyer to control the tracking of our asset, and follow-up after 14 days regarding the status of our asset (i.e., "have the infringer(s) replied?").

Log any information from the lawyers of our asset into the CMS.

The Sales, Document Production Admin, & Legal team are all involved in the process of our asset, except CMS (they will only do software changes for law firms databases)

Sales Team - communicates with the clients how much data (i.e., IP names & addresses) has been sent to the lawyers and the progress in the courts.

If they have a question about a contract? who do they approach?

The Legal Team

Document Production Admin Team - assisting with turning the infringements into paper, which then gets filed in the courts.

they will also get the paper information (i.e. IP names & addresses) back into the CMS.

Legal Team - will assist the lawyers/law firms with the legal issues,

- how to handle opponent council
- they will create the legal documents (i.e., the motion of expedited discovery, demand, and settlement agreement letter).
- they will assist the Sales Team to close their deals
- if they have a questions about APMC's product? who do they approach? The Sales Team per US district territory (i.e., TAR breaks down the # of infringers for each separate state district).

it shows the list of the lawyers & where they have jurisdiction based on the specific US territories.

check the "chain of title," to make sure APMC has the rights to proceed.

CRM (Podio)

- CRM is process tool that BPO Cebu Office will use to do the sales process.
- CRM is on Podio & has template contract agreements.
- CRM has a template library showing sample contract agreements.

Once we have the exact client information, we send it over to the lawyers.

Title Allocation Report (TAR Analysis)

It's an Excel spreadsheet.

It's circulated by email.

Usually 2 different reports

- a World wide report
- a US report

The results that the data gathering team gives back.

It basically shows a list of clients representing the following:

- the rightsholder
- the title
- the title ID
- start date
- end date

The figures (i.e., the # of infringers for a particular movie title) for the US in (total).

How does TAR analysis assist APMC?

It shows the total # of infringers of each movie (in descending order)

It helps APMC know which movie is being most pirated per country, state, territory, or district.

It allows an assessment to determine if APMC has the rights for this movie based on the specific territory.

It allows APMC to decide which department or team gets specific data to be allocated to complete submitting to the lawyers.

It shows the list of the lawyers & where they have jurisdiction based on the specific US territories.

Check the "chain of title," to make sure APMC has the rights to proceed.

Then, draw down into the detains, using the Abocado software.

What are the tests that APMC performs to decide whether or not we proceed with the title? (i.e., the "Chain of Title" steps)

1. Does APMC have the rights?
2. Does APMC have the lawyer? (i.e., in the right state to license to practice where APMC wants to file).
3. Does APMC have the sufficient number of infringers in a particular swarm?

NOTE: These are the 3 things to think about, when APMC says it's time for a "data drop" to the lawyers (i.e., usually data drop delivered every 2 weeks).

How do we find a list of lawyers?

1. Go to Podio
2. Click USA APP
3. Click Attorneys APP (i.e., it's a reference field for all of APMC's attorneys)
4. It's sorted by US territories.

NOTE: I need to make sure I include all the relevant contacts (i.e., lawyers & assistant lawyer within the law firm) email information for each. Why?

Podio shows or lists all the key people I need to send the data to.

NOTE: Check the "Comment Section," & click the "Territory Comment Section" to get additional information.

Why might Podio show that a lawyer is retired?

A lawyer may be retired because possibly the district or the territory doesn't like multiple paperwork of joint lawsuits.

Services

- Deliver to the law firms
 - Keep track of the law firms
1. The Recovery Program - to do the data monitoring to find the infringer(s)
 2. The Digital Millennium Copyright Act (DMCA) - a letter to send to a particular website, (i.e., youtube) to take down our client's content from that site

Newsletters

What are the tasks of the Document Production Admin Team?

Task 1:

- to complete a "Complaint Generation Letter" document for the lawyer (usually 10-12 pages).
- this is how APMC makes most of their money
- use "Book Mark Wizard" (i.e., predefined book marks)

Task 2:

- change the format (i.e., font, text, size, spacing, etc.,) for lawyers needs or requests.
- based on U.S. territory rules & regulations

Task 3:

- perform any data entry and data import needed for the client.
- actual case management (input information using Abocado software templates)

Task 4:

- record or put replies over proper record keeping (i.e., call notes)

Task 5:

- send email, if no response after 7-10 days.

Task 6:

- assist with opponent council (i.e., an "infringer(s)" give the case to his/her lawyer)
- Sometimes, a settlement, or payments (\$) will appear...

Task 7:

- create a "Settlement Agreement" document (i.e., the "infringer" will stop & APMC is comply with it).

Task 8:

- create a "Dismissal Final" document (i.e., send to lawyer, & he will submit it to the court to communicate the case is settled).

Task 9:

- APMC may have BPO Cebu Ofc. complete & send out a Digital Millennium Copyright Act (DMCA).
- also complete the YouTube Content ID statement.

Steps for starting a case (Stage 1)

How do I start a case in court?

Step 1

You file a "Complaint Letter" document to explain the following:

- it tells the court what our grievance is.
- it tells the court someone has been stealing my copyrighted work without paying for it.

(This 1st step sets into motion the legal process)

Step 2

Create a "Motion for Expedited Discovery" document, which explains the following:

- this allows APMC to get the infringers ISP's names & addresses.

Why do we need these documents?

It tells a story to the judge & persuades him to grant an order, ordering the ISP's to provide APMC with the information so that we can persecute the infringers.

- BPO Cebu Office Role: to create steps 1 & 2 documents for the lawyers.

Step 3

When the order is granted, the ISP's are served with the order (i.e., the judge will demand the information from the ISP's & give to APMC).

Step 4

- BPO Cebu Office will be responsible for service process & produce the documents (i.e. a subpoena, or a request for a production of documents)

Step 5

- BPO Cebu Office will produce all of the information (i.e., step 1, 2, & 4 documents) into a neat packet for the lawyers.
- usually the period of reply is approximately 30 days.
- if after 30 days, there's no reply from the ISP infringers, the BPO Cebu Office will be chasing the ISP's, (i.e., we'll be preparing the chasers in the name of the lawyers & complaining to the ISP's why they haven't send the requested subpoena information).
- this BPO Cebu Office roles of steps 1-5 will be a big help for our lawyers.

Step 6

- once the BPO Cebu office receives all the ISP's names & addresses, a "Demand Letter" will be send out:
- saying to the "infringers" your internet connection was used to infringe, & here is a settlement offer stating (do you deny or contest this letter).
- BPO Cebu Office will produce this letter using Case Management Software (CMS), and this process is called "Subsequent Correspondence Management."
- Subsequent Correspondence Management is used to identify appropriate responses & draft response documents to the lawyers.

Step 7

- the BPO Cebu Office will produce settlement documents:
- settlements takes place when the infringers wish to settle.
- in order to wrap up the settlement, the BPO Cebu Office will produce a "Settlement Agreement" document, using CMS.
- finally, it will be sent to the lawyer to complete the process.

Steps for starting a case (Stage 2)

What does APMC do if any infringer(s) refuse to settle?

Step 1

BPO Cebu will put those infringers into a special database (i.e., Monitoring System 2)

Step 2

BPO Cebu will have someone analyzing the IP names & addresses.

Step 3

BPO Cebu will select suitable targets to litigate individually.

What are the early stages to prepare for an Individual Lawsuit?

Stage 1 - BPO Cebu Office will take a target approach in determining an individual lawsuit.

Stage 2 - APMC doesn't just file a lawsuit from any IP address they find.

Stage 3 - BPO... will conduct a due diligence or an investigated approach for an IP address

Stage 4 - BPO will determine who does it belong to.

Stage 5 - BPO will determine which ISP it is.

Stage 6 - BPO will determine what are the connected infringements in monitoring system 2 (i.e., can we find who's associated with that IP address).

- Monitoring system 2 allows APMC to profile individuals based on their download history

Stage 7 - Using the monitoring system 2, BPO... will select individuals who are wealthy and are likely to settle & put those in an individual lawsuit.

Stage 8 - This allows APMC to get the return on their investment (i.e., the \$400 costs involved to file for every individual lawsuit).

What is the difference between an individual and joint lawsuit

An individual lawsuit represents a single individual, whereas a joint lawsuit involves more than one person.

Regarding U.S. Legal System:

- In some states, APMC can only do individual cases, but in other states we can do both individual and joint lawsuits.
- The cost to file a lawsuit in the U.S. is usually \$400.
- Which lawsuit, individual or joint is more cost effective for APMC?

A joint lawsuit, because we only file the \$400 fee for one case, whereas an individual lawsuit has to file \$400 for every individual (i.e., it's expensive to file)

- APMC's goal: the more individuals that can be contained within the lawsuit, the more cost effective for the company.
- BPO Cebu office can handle individual lawsuits with multiple filing documents (i.e., 50 individual documents to control effective costs).

What are the essential functions of the Case Management System (CMS) development team?

- they provide 1st level support for all other departments regarding information technology issues (i.e., the IT team is here to make life easier).
- they provide all other departments with adaptability & ease of APMC's various IT software.
- they provide "change management" issues (i.e., tracking incidents, problems, requests, error handling, etc.).
- assist the Document Production Admin team with 1st level support (i.e., basic errors).
- they provide data base management for every unique APMC's lawyer firm data base given to APMC (i.e., backup, permission, & user management).
- they develop other tools in addition to CMS (i.e. Administration tools). - i.e., infringement over ebay

What kind of copyrights does APMC focus on?

APMC focuses on movie rights.

How is this accomplished?

- the license allows you to distribute for a specific time period (i.e., 5 years).
- APMC cannot enforce, if the word "exclusive" is not written in the client's copyright document.
- if it is a "distributor copyright," then it has to be "exclusive copyright."

The Sales Agents divide the copyrights into 2 different ways:

1. Give someone a license (i.e., an "Exclusive License" only done in an exclusive territory).
 - APMC can only enforce "exclusive" copyrights written in the client's copyright document.
 - Option: APMC may attempt to gather all of the copywriters, but it's too expensive for APMC.
2. Give someone an assignment
 - this assignment is a sale for the rights of an individual or company to keep the copyrights.

What is the difference between a copyright license and copyright assignment?

A copyright license allows you to distribute the movie for a certain time period, whereas, a copyright assignment allows an individual or a company the right to keep the copyright.

Important Note: APMC cannot file a lawsuit, if the client does not own the copyrights of the movie!!!

What are the functions of the LEGAL team?

- assist with the lawyers & law firms (i.e., consulting).
- diagnose problems and issues.
- offer solutions.
- perform "front office" duties (i.e., like Client Management)
- perform "ad hoc" work (performed mainly by Dan Miller).
- responsible for exploring new territories.
- finalize the initial sales team deals with new client (i.e., the legal and sales teams coordinate together to complete the process).
- make basic status calls (BPO Cebu Ofc.) to keep the relationship alive & consistent.

How Do We Start a Lawsuit in the US?

- APMC does not deal with Criminal Cases (that require 100% of evidence to prove guilty).
- APMC only deals with Civil Cases (that only need 50% of evidence to prove guilty).
- We let the court know that you have a complaint.
- it sets out the grounds of what I'm complaining about.
- the 1st document that we send out is the Complaint Letter:
- it reveals the remedies that we're after (i.e., damages, injunctions...)

What is a Prohibitory Injunction?

An injunction that stops someone from doing something else.

What are damages (in legal terms)?

It's compensation for the client (i.e., to pay lawyers & other 3rd parties)

What are statutory damages?

a willful infringement ranging from \$2,500 - \$150,000 (for an act of copyright infringement).

A real life settlement is around & \$2,500 - \$7,500.

What is APMC's role with the Prohibitory Injunction?

- APMC is trying to get enough injunctions against a particular Bit Torrent swarm infringers.

- Usually, most infringers settle & turn off their Bit Torrent & stop distributing our client's copyrights work.
- once you get to a certain stage, the swarm stops being efficient.
- this gradually reduce the members within swarm.
- this is the ultimate aim of an injunction.

Podio

1. Basic Information of Podio

- has building APPS or existing APPS, and free APPS which can be created (Note: APMC wants everyone to know the basics for APP building).
- is a social network (i.e., Facebook), but it is for "In-House"
- no programming needed, it is very user friendly.
- allows APMC to make improvements or suggestions.
- organize taxes, work space, etc.
- is very flexible, manages people, charts, task manager.
- allows APMC to organize, communicate, & get work done.
- APMC NEW POLICY WANTS EVERYTHING DONE ON PODIO TO MAKE THE WORK PROCESS TRANSPARENT.

2. Podio Introduction Video

- most of the work related communication will take place on Podio.
- helps APMC to structure workspace (i.e., it will give a specific group of people a task to function a common goal).
- assists with the tracking of work tasks, either specific steps, progress, or completion of documents.
- helps everything to be in the right section or workspace.
- eliminates frequent email use.

3. Podio Task Tutorial

- is one of the big things the BPO Cebu Office will be using.
- many categories, such as "My Tasks," "My Delegated Tasks," "My Completed Tasks."
- a task can be created by clicking the "Assign Task" button.
- Podio tasks are conceptualize on what I'm working on.
- Podio allows others to see what the task is about & how it fits in with the whole project.
- can be used to send "emails" as "tasks."
- labels can be added to tasks (i.e. as a timesaver).
- my PODIO tasks can be grouped by "Due Date."

- can also be used via a cell phone for those "on the go."

4. PODIO (How Work APPS are Built)?

- the simplest way to start an APP is to think of the structure of an APP similar to an Excel Spreadsheet.
- when you build an APP space on PODIO, everyone can use it.
- the PODIO "building blocks" are like the "columns" for an Excel spreadsheet.
- the PODIO "items" are like the "rows" for an Excel spreadsheet.
- categories can be created on an APP, such as (Not Started, Working On, & Complete)
- Multiple APPS can work together to get work production done in a more efficient & effective manner.
- on the bottom of the APP shows how your APP will look & how other people can interact with the APP.
- the APP function has "Advanced Settings," explaining how you want your APP to appear.
- the APP can filter to give me specific information.
- PODIO allows me to link APPs together by clicking the "Modify APP" button.
- APPS can be used to get everything down in the project (i.e., to see the big picture).

5. PODIO Filter Tutorial

- Podio allows me to create a report for a specific field (i.e., Recruitment for IT technicians only).
- Podio can also assist with various APMC documents that BPO Cebu Office will deal with on a daily basis.
- To identify the filter, look for the "funnel cloud" icon on the top of the screen.
- Podio can also be used to filter specific fields for statistical data information.

6. Podio (How to Store Documents Tutorial)

- When a document is posted, it's very important that the document get's posted in the right workspace & APP.
- Whenever a document is revised, APMC requires the following filing and version format:
 1. (FileName)(Date)(Version#) for example: WhiteCompanyComplaint011013V1
 2. The date should be the last edited date and the version should be the most recent version.
 3. No spaces between the file name and no dot (.) in the file name.
 4. Do not change or "rename" file names, just change the version #.
 5. Use the "comment field" for any additional information (i.e., "this is a rough draft red line version, do not use").
 6. Everytime a document is revised, especially on the same day, change to version (i.e. V1, V2, V3, V4, ...)

What are the steps to change a document on Podio?

1. Pull the document out of Podio.
2. Make the necessary revisions.
3. Save the revised document with the latest version# (i.e., V3).
4. Put the revised document back into Podio.

7. Other Podio Tutorials (See YouTube videos)

How to Share a File?

The file can be uploaded directly to a Podio workspace or APP.

How to Export Data (i.e., drag & drop)

- Also can send a link form (i.e., Podio can assist in creating a URL illustrating:

How to Setup a Web Form Feature?

- ISP addresses
- Names & addresses of individuals
- Notes to customize within the settlement agreement (i.e., outside of the standard law firms template)
- the web form assists in interacting with the clients.
- Whenever you want a settlement agreement form, please "Fill-in" the information using the Podio web form.

How Can Podio Be Used to Track Copyright Documents?

APMC uploads the documents so that they can be accessible at anytime.

i.e., if a new US lawyer represents a new territory for a movie client, then the BPO Cebu Office can use Podio client files to:

- for that movie, Podio will assist in knowing who the client is, by clicking the sales agents or movies icons

For each movie section, there will be a section showing client information, such as:

- Name of client
- Title of the movie
- Territory claims of which rights the client has the rights to (i.e., you can click on Podio the different territories the client has)
- Comment section: if BPO Cebu Office has any comments or questions about the client.
- Document files consisting of:

1. Client Chain of Title

BPO Cebu Office needs to check if it is "complete" or "incomplete."

The client will have a chain of title when they have the following completed documents:

1. Anti-Piracy Contract Agreement
2. The Motion Certificate or Copyright Registration Certificate

2. Client Copyright Registration Certificate

- This proves whether or not this movie has a registered copyright, (i.e., with the US copyright office).
- This proves that our client is the sole copyright owner, so the opponent will have prove that the client is not the owner.
- APMC only works for clients who have a valid copyright registration certificate.
- If the client is high profile, & the movie is highly pirated, but they don't have a certificate, then APMC will obtain this document & send to the client to complete the steps to get this certificate in order to enforce.

3. Anti-piracy Contract (i.e., who has the rights, the territory, terms, etc.)

4. Corporate Disclosure Statement - What's the meaning of this document?

- It reveals which parties are interested in the lawsuit.
- It goes into details of the ownership structure of the Production Company.

If a client asks, "Why do you need this document?" just use the Podio Sales Q & A to give them the answer.

Note: If APMC doesn't receive it in a reasonable time, i.e. 10-14 days, contact to follow-up with the client.

What's the reason of a Corporate Disclosure Statement?

1. It's one of the required documents that sets down in the Federal Procedure Rules.
2. It allows the judge to view the document to avoid any conflict of interests, of whether he'll take the case or not.

Other important tasks regarding APMC client contract information using Podio:

- Check the distribution agreement on Podio to confirm the specific US territories.
- In the "Comment Section," we will find a basic analysis of the chain of title to confirm that it's all OK
- Sent out confirmation to the lawyer (i.e., all of the Podio information, such as the movie client, distribution agreement, & comment section analysis)
- This is BPO Cebu Office's work, please confirm it, yourself.

Overview on Podio Training

Podio is APMC's collaboration tool

All of the Sales Team procedures is reflected on Podio.

You can set up a quick task or assign a task to anyone to be completed today, tomorrow, or whenever you specify to task completion.

With Podio, we can attach files, such as Word doc, PDF, Adobe, either by "drag & drop," or the open a file to attach.

It's important to always attach the right workspace on Podio (i.e., Employee Network, CRM, Internet/HR,...).

We can share it with other employees or keep it private.

We can create a reminder, if the date is in the future.

Usually, APMC requires a very detailed task description, so that all colleagues can quickly understand all the relevant details or facts about the task.

Podio has filter possibilities, where you want to see only specific information (i.e., Canada only, or the Pacific territory section of the US).

The APPS will appear on the top or bottom on the Podio page.

Podio has many workspace or categories on the left side, such as (Employee Network, Abocado, CRM, DMCA, & Internet/HR).

Podio basically removes email to make communication more time effective & eliminates miscommunication of sending emails back & forth. Podio can do it in 1 step.

Whenever we encounter problems or bugs, it's important that we give as much information as possible, so that the IT Team can quickly determine & fix the problem.

For example, give the Abocado version, which module was I using, when did it happen (date), the steps leading to my bug or error, & we provide screenshots of the error messages.

Regarding screenshots: there's a tool which is more effective, (i.e., taking a video of the error message from the computer screen).

This allows the IT Team to see exactly what occurred, or the steps that triggered the error message.

It's important to provide detail or specific information of the clients for you & coworkers.

Podio Information for CRM Tool

In the future for APMC, www.usabit.com information no longer gets inserted in a Word document, but rather, on a Podio APP. Why?

The reason is that APMC already has the lead on the APP in Podio.

There will be CRM tasks for an individual or the team that need to be completed (i.e., Angel complete the report...).

The CRM APP is the database that is storing all the clients.

The CRM has many categories or APPS on the top of the Podio page (i.e, Activity, Address Book, Clients, Movies, Communication, Leads, Deals, Partners, Sales Q & A, Templates, and Add an APP.

Each of APMC client has their movie in the "Movie APP" file.

What's the difference between "Clients" and "Movies?"

Answer: Each movie requires all of the requested paperwork or documents (i.e., the chain of title documents), whereas the client APP gives client contact information, such as names, addresses, phone numbers, territory, etc.

What's the difference between "Clients" and "Leads?"

Answer: A client is already working with APMC with a signed contract, whereas a lead is a potential client with no signed contract to date.

When APMC does a lead with a potential client, the perfect deal would be when the client immediately works with APMC & gives all required documents promptly.

In the real world, every potential client has many questions, concerns, or issues, so the Podio CRM has a category or APP called, Sales Q & A, where there are many answers already in the Podio database for the Sales Team to consistently use to give a response to potential clients.

Podio Information on How to Build an APP

We can add an APP to do a www.usabit.com check

There are 2 ways to build an APP: (look for the command on the right-hand side of the Podio screen).

1. Can go the APP Market where they have predefined APPS (i.e., already built in APPS to give me suggestions on possibly choosing one), or
2. We can go the the "Build a New APP" section to create my own APP.

To build one from scratch or create a new APP i.e., usabit APP, do the following steps:

1. Create a task (i.e., on a daily basis, we go on this website).
2. Once on www.usabit.com, when we see a movie being pirated, so we gather the information that is needed for the APP
3. To find out more information about the movie client, we search on www.imdb.com

4. We gather the information & input it on a Word document, (i.e., title of the movie, the rightsholder, the contact details, the production company, information about the downloaded website, and the imdb web link).
5. We create a "text box" APP for the movie (i.e., label it "title of the movie").
6. Use a "symbol" (i.e., \$) to identify what the APP icon will look like.
7. Next, we need another text box to create (i.e., "name of the rightsholder", using a single line of text for a few words)

It's best to put the rightsholders in the "Address Book APP," so that the www.usabit.com folder can link back to the rightsholder

Reason: this allows us to know that we contacted the movie client (i.e., about your other 5 movies that been pirated, here's your 6th movie being pirated, "do you not care?"

8. Another text box for the "contact details"
9. Another text box for the "production company"
10. Another text box for the "downloaded website link"
11. Another text box for the "imdb link"
12. Create a category field box for the email (i.e., "Respond" "No Response").
This helps us to extract the information & load it into the mail check.
13. Create another category field, (i.e., "Not Interested" "Interested").
The reason for 2 categories is so that we will know what we'll going to be following up on.
14. Another text box called, "Interested," with the text, "Yes/No" (i.e. set the field for only "one choice")
15. Create an image box (i.e., from the image from the website).
16. Create a notes box on the very bottom of the APP (i.e., any relevant notes pertaining to the client).
17. Steps 5 to 16 should be "required fields"
18. The end result looks like a form, where we can input all the required information.
19. IMPORTANT: To put it in the right section or workspace (i.e., CRM, not Internet/HR).
20. The Manager or whoever created the APP can assign a task to different team members to complete each part of the APP create (i.e, Angel find a movie; Rhea find more information on www.imdb.com; Ken to find contact details,...)

Other Important Podio APPS

The Internet/HR APP

- i.e., if I want to take a leave of absence

Use the Vacation APP, when I want to take some leave.

Use the Absence APP, when I'm sick.

The Procedures APP

That's where the Staff Handbook will be stored

Other Important Podio Information

Podio suggests to create a "daily task," not long-term tasks.

The reason: there should be "actions" in the tasks to be completed.

Just create a "task" for the daily action or short-term to be completed for an individual or groups of people.

IMPORTANT: Any import/export of Excel, needs to be completed by an IT Team person (i.e. Charity).

Podio has a "Calendar" APP to organize important meetings, tasks, etc. to be completed in the future.

Podio has a "TAR Analysis" APP for information regarding title allocation report & other analysis information.

Podio allows you to customize any APP or category in the home screen (i.e., according to any APP that you access regularly).

Anything a team member wants to create, should create a "Test Workspace" APP (i.e., just PRIVATE for myself) in developing a new APP.

- but before it goes "live" (i.e., everyone can see it, team members, clients, lawyers, etc.), we need to get it approved by the manager Tom.

To bring people into conversations, we select them to join in the task or project.

Tip: don't invite people into conversations who don't really belong to the task.

Tasks in a workspace can be "Public," but also some can be "Private," (i.e., just between 2 team members).

Another useful tool is the "Labels" (i.e., label your tasks with a specific marker to highlight an "urgent task").

It's a good way to checking off your daily task list (i.e., a bucket list) to see what was completed, not completed, etc.

For short-term things to be completed, it's best to create a "task" on Podio.

For long-term projects to be completed say, in 6 months, it's best to create an "APP" on Podio.

On Podio, we can do a "Video Call" to talk with someone.

Podio give us a real easy way of extracting data (i.e., an Excel spreadsheet), use the "Import/Export" button.

For confidentiality reasons, not every APP will be available for all team members, only those to who it directly effects their job tasks.

YouTube Anti-Piracy Procedures

Information RE: Section 512(c)(3)(a)(i.) to (vi) and procedures to report copyright infringement:

APMC focuses on rights of a production & distribution to go for the copyright itself.

Part 1: Reporting to YouTube Copyright Infringement

Submit the form, "Copyright Infringement Notification" to youtube to remove copyrighted material.

Submit a "Declaration" under penalty of perjury that the person submitting the notice does so with the authorization of the copyright holder.

There are statutory penalties 512(f) for making misrepresentations of the "take down notice."

There is no obligation of the person serving the notice to take any formal legal proceedings against the alleged infringer.

Part II: Counter Notices

What happens when YouTube receives a take down notice?

1. They are under statutory obligation to remove the video, expeditiously.
2. They are also obligated to notify the person upon whom the notice was served.
 - This person has the option of whether of not they wish to serve a "counter notice."

What are the requirements of a Counter Notice?

1. Following the procedures of Section 512(g)(3)
2. If a counter notice is served, they must send this notice to the person who originally sent the take down notice.
3. Unless they are informed, the formal legal proceedings have been issued, then they should restore access to that video between 10-14 days, after receiving the counter notice.

What needs to go into a Counter Notice? (i.e., what forms does it take?)

You cannot serve a counter notice directly from a youtube page, why not?

The counter notice has to include your name, address, & phone number.

And youtube under statutory duty to disclose a copy of the take down notice to the person who issued the take down notice.

This is per the requirements of the Digital Millennium Copyright Act (DMCA)

How long does it take for the counter notice to take effect?

visit: chillingeffects.org (i.e, the link is in the description)

it contains useful information on the DMCA

Helpful guidelines on how to complete the counter notice

A link to the specific page you want is in the description.

If you fill-in all the boxes, it will generate a standard letter for you.

All I need to do is to add the detail(s) of the relevant video(s) unto a separate sheet of paper.

The best way of identifying the information is by using youtube's own numbering system (i.e., URL).

What are the 3 ways to send the counter notice to YouTube?

1. Having done that, I can FAX the letter to youtube, as the address & FAX number is in the description.
2. I can scan it into the computer and email it to youtube.
3. You can also "Post It" to them.

NOTE: It is recommended that you do all 3 ways in sending the counter notice to youtube.

NOTE: If you do not live in the US, this process will NOT work. What can BPO Cebu Office do?

1. Go to the chillingeffects.org website on the recommended page
2. Complete the form, as if I were living in the US.
3. It will then generate a letter for you.
4. I will have to amend the letter by removing the 2nd paragraph, related to jurisdiction.
5. Replace it with the paragraph contained in the description.

What is the usual reply time for YouTube to respond?

Do not expect youtube to respond or act, with the same expedition in responding to your counter notice, as they do with a take down notice.

Experience will show that youtube will not respond.

It is worth chasing after their legal department after a few days to ensure that they have receive your counter notice, and that they are acting on it.

If it does not comply with the statutory requirements, youtube is likely to ignore and not inform you about it.

Note: DO NOT TAKE THE ABOVE CHILLING EFFECT DESCRIPTION AS FORMAL LEGAL ADVICE!!!

APMC, usually, do not receive many Counter Notices

For further information on YouTube content information, go to: www.youtube.com/t/contentid

What is a Complaint or How do you file a lawsuit in the US?

You let the court know that I have a complaint in the US, and I want the court to do something about it.

NOTE: There's a separate document that goes with the complaint called a "Motion for Expedited Discovery.

What are the relevant things to note on completing the 1st Document, or the complaint letter? (i.e., when editing a complaint letter)

1st - identify & edit the district, (i.e., Northern District of Ohio)

APMC has the software that should automatically change things for you, but be responsible to check for proper lawyer territory.

2nd - identify & edit the correct client

- go through the chain of title documents
- determine who holds the rights (i.e., does my client own the rights to sue)
- Example Client Name: Knights of the Templar llc (i.e., the production company who owns the copyrights)

3rd - identify & edit the correct address

- the address of the copyright owner
- the registered business address
- the address should be on all the agreements that we're analyzing
- when in doubt, always go back to the copyright owner & ask for the correct address

4th - CA (i.e., the case #)

- before we file a complaint, we don't know the case #, so we leave BLANK.

5th - Judge

- we don't know, so we leave BLANK.

6th - DOES (i.e, unknown names)

- there called John Doe defendants because there people that the plaintiff wants to sue.

What are the fields that change in a complaint letter? (i.e., they will be highlighted)

- the plaintiff's name
- the plaintiff's address
- the district territory
- the DOES (i.e, 1-20)

The 1st Section is called the Complaint (Reference from Training Documents File: Complaint 081112)

- it tells the judge this is a suit for a copyright infringement, under the US copyright act.
- the 1st paragraph is explaining why its proper to file a complaint.

The 2nd Section is called the Jurisdiction & Venue

1st paragraph:

- were telling that venue in this paragraph its proper
- based on these sections of the US Civil Code
- we tell the judge that the defendants are unknown at this time
- however, based on geo-technology, & upon information & belief, each defendant may be found in this state.
- What is geo-technology & why do we use it?

Answer: Using an IP address, we can learn the location using geo-location technology.

2nd paragraph:

- now reveals to the judge that it can rule over the people (i.e., the DOES defendants).

3rd Paragraph:

- we're saying that the court has jurisdiction over the defendants due to geo-technology places all defendants within this state.
- paragraph 3 reinforces paragraph 2 by giving it more detail to the explanation of paragraph 2.
- upon information and belief, all DOES or defendants reside in the state and within the preceding district.

The 3rd Section is called the Joiner

- an explanation to the court why we joined all these lawsuits into 1 lawsuit
- paragraph 4 says DOES or defendants "true identity" are unknown at this time.

- we don't know who these people are, but they acted collectively
- & acted interdependently (i.e., everyone is interrelated by internet connection).
- paragraph 5 reveals the "swarm" (i.e., a file sharing that can be identified by a file hash)
- each defendant illegally "uploaded" & "shared"
- why are we focusing on "uploading?" Answer: people who are uploading files causes more damage by distributing the files to others.
- paragraph 6 explains basically "willful intention" or they knew what they were doing.
- paragraph 7 key section, because the legal test for "joinder" is that these uploading transaction(s) are occurring in the same swarm.
- paragraph 8 explains the Peer-to-Peer (P2P) process.
- paragraph 9 reveals highlighted text that needs to change from court to court
- here we introduce the idea of a "hash" (i.e., this is the hash value assigned to this version of the title & loaded it into the BitTorrent client.
- i.e., hash tag information: SHAL:B678D7812
- paragraph 10 tells the "sharing" of the hash values from computer to others to make immediately available to all other DOES or defendants.
- paragraph 11 makes the distinction between distributing & copying.
- paragraph 12 is discussing about the swarm viral spreading
- paragraph 13 reveals that the defendant's distribution of a single unlawful copy will cascade (domino effect) and result in a world wide distribution of that copy.
- paragraph 14 to further explain the interacting of swarm infringement occurring in this district that the judge is responsible for.
- paragraph 15 explains the whole critical mass concept
- paragraph 16 explains the Peer-to-Peer (P2P) exchange
- paragraph 17 explains the Distributed Hash Table.
- paragraph 18 reveals that the torrent swarm consists of numerous individuals, working together to infringe on plaintiff's copyrights.

The 4th Section is called the Parties

basically it explains all the individual(s) or groups that are involved in infringement of plaintiff's copyrights.

- paragraph 19 defines the plaintiff or gives the company details
- paragraph 20 defines the defendant(s) or gives information of the infringers (i.e., by hash identifier number)
 - Note: the reason we define plaintiff & defendant is to narrow it down (hash identifier number), otherwise, the judge will not be happy.

- paragraph 21 explains that the hash file provides access to an unauthorized copy of plaintiff's copyrighted motion picture.
- paragraph 22 reveals that the plaintiff's copyrighted product is a marketed, produced, & commercially salable product (i.e., to prove revenue).
- paragraph 23 this tells the judge what the plaintiff wants (i.e., redress for rampant infringement of it's exclusive rights of motion picture).
- paragraph 24 similar explanation to paragraph 23.
- paragraph 25 explains that we're introducing to the judge an exhibit
- the exhibit includes: IP addresses, date & time of infringement, ISP, the Torrent file, & the results from the geo-location IP technology.
 - NOTE: The BPO Cebu Office will be drawing down on the data using the TAR analysis (i.e., using the TAR analysis tool function, we analyze the data, & the results of all of that analysis ends up as "Exhibit B," in one of these complaints.
- paragraph 26 is basically telling the judge what we need (i.e., IP addresses now, to learn the true identity of these DOES).
- paragraph 27 explains that plaintiff believes that information obtained in discovery will lead to the identification of each DOES true name & identity.
- paragraph 28 explains that it might not be the account holder, but we'll find someone, within the household who's responsible for infringement.

The 5th Section is called the Statement of Facts

- it deals with the legal tests needed to issue a copyright claim.
- it answers the question: What do we need to satisfy the judges that we have a standing (i.e., a right) to bring this copyright claim.
- paragraph 29 we're saying that our client owns the "exclusive" rights to the motion picture, under US copyright law is the original & copyrightable.
- paragraph 30 deals with, "How?" we demonstrate paragraph 29. (i.e., Exhibit A - The Copyright Registration Certificate).

Why is the Copyright Registration Certificate important?

This means we don't have to prove all of the things of copyrights, we just produce the copyright certificate, and its assumed, that you have the copyrights to the motion picture.

NOTE: APMC will NOT file a claim, unless we have the Copyright Registration Certificate!

- paragraph 31 we're saying that our client owns all the rights (i.e., see the Copyright Registration Certificate).
- paragraph 32 reveals that the copyright owner has the "exclusive" right to reproduce the work.

- paragraph 33 basically is telling the judge that the defendants knew what they were doing (i.e., they had notices everywhere, it's no secret).
- it deals with the legal tests needed to issue a copyright claim.
- it answers the question: What do we need to satisfy the judges that we have a standing (i.e., a right) to bring this copyright claim.
- paragraphs 35-55 is repeat information from the above sections of the Complaint.

The 6th Section is called the Direct Copyright Infringement (Count 1) (i.e., the infringement of an "exclusive" right)

- paragraph 56 this is the infringement of the direct rights that the plaintiff has under the copyright act to reproduce the motion picture & to distribute the motion picture to the public.

How are we going to seek an injunction?

An injunction stops someone from doing something

Result: The plaintiff is asking for the damages that the DOES are causing, which is great, continuing, and irrevocable.

- in other words, the DOES are continuing to cause irrevocable harm, & that's the basis for the injunction in a BitTorrent context
- so the plaintiff is asking the court to prohibit each DOE or defendant of further infringing activities.
- we're also ordering that each defendant destroys all copies of the motion picture, because they never paid for it.
- (Count 2) - is the Contributory Copyright Infringement
- it explains that's a violation of the "exclusive" rights to reproduce the motion picture & distribute it.

What's the difference between Count 1 & Count 2?

- Count 2 is not saying that you have distributed it, rather you've acted collectively, in a swarm together to infringe = contributory copyright infringement.
- Count 2, basically, is willful, intentional, & complete disregard to the plaintiff's copyrights.

Wherefore, Plaintiff prays for judgment against each defendant, is really a summary of what the plaintiff is after...

Part A - "prayer" is a preliminary and permanent injunction to prevent the defendants from distributing the work, destruction of all copies, unless they have a lawful license to distribute the work, destruction from all computers.

Part B - for actual damages and statutory damages at the election of the plaintiff.

What's the difference between actual & statutory damages?

Actual damages relate to the proven actual harm or damages that has been caused to the plaintiff, whereas statutory damages doesn't need to be proven.

APMC always goes for statutory damages because of the range (\$2,500 to \$150,000).

- the plaintiff also asks for the cost in pursuing the defendants, the attorney fees, and whatever fees the court deems proper.
- BPO Cebu Office will need to change the plaintiffs (rightsholder) name, the attorney's registration number, address, email address

- *** THIS ENDS THE COMPLAINT LETTER ***

What are the relevant things to note on completing the 2nd Document, or the Declaration or Affidavit? (Reference from Training Documents File: Affidavit CBS 081212)

- is basically a statement that declares that what the Plaintiff is saying is true under oath.
- NOTE: the BPO Cebu Office will be responsible for generating the affidavits for each movie.
- there needs to be a "Declaration" for every expedited motion of discovery.
- every document packet (i.e., data drop) has to have this affidavit attached to it.
- presently, APMC is using the affidavit long form (i.e., 11 pages), but it repeats many of the things that are in the Complaint letter.
- sometimes, APMC has to write supplemental declarations to satisfy any sort of questions that the judge may have
- BPO Cebu Office will be receiving these declarations from Daniel Macek
- this declaration supports motion for expedited discovery, or telling the judge we need this information now.
- paragraph 1 is a serious declaration that's stating everything is true & accurate.
- paragraph 2 in regards to software consultant (i.e., he can talk about software issues), & we're hoping the judge won't question his qualifications too much.
- paragraph 3 we're basically saying that the "Internet" can be a great place to network with each other.
- paragraph 4 explains that the "Internet" can be use to negatively give opportunities of wide-scale infringement of motion pictures
- paragraph 5 reveals that once a motion picture has been transformed into an unsecured digital format, it can be copied further & distributed over the internet.

- paragraph 6 explains the Peer-to-Peer (P2P) network & its processes of copyright infringement.
- paragraphs 7-11 further explains the P2P processes (i.e., or the sequence of pieces in downloading a motion picture into one complete file)
- this declaration of affidavit adds credibility, because its coming from a different person, and therefore, reinforces the complaint that's been drafted
- paragraph 12 reveals that all infringers connected to those files are investigated through downloading a part of the file placed on their computer.
- paragraph 13 to break this process down, what are we capturing from these infringers that our monitoring system is connected to?

IP addresses, the hash tag, the time & date of the infringement, but the most important thing we're capturing is that we have a "packet sniffer" (i.e., that captures all the network traffic that is passing through the system.

- paragraphs 14-30 explains about the IPS processes, including the processes of the IP steps of infringement
- paragraphs 31 explains the BitTorrent piece by piece process in the correct position of the downloaded file (i.e., to prove that the software does it automatically)
- paragraph 32 is about the locator process of looking at various data bases to get as much information from a IP address in a language that the judge can follow.
- paragraph 33 reveals that the users distributed the files (in the district where the judge presides), but also, where the specific location took place.
- that completes the declaration of affidavit

What is the key part, or what is this infringer actually doing?

The infringer is confirming that the downloaded one is the same as the original one, and the piece that was downloaded from the infringer is the same as the piece that belongs in the downloaded file.

What are the relevant things to note on completing the 3rd Document, or the Order on Motion for a Leave to Serve Third Party Subpoena Prior Rule 26(f) Conference?

this is setting the legal basis for the judge to order this motion.

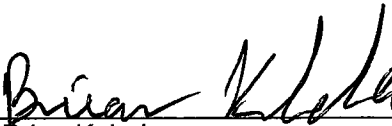
What are the relevant things to note on completing the 4th Document, Motion for a Expedited Discovery?

See information similar to the Complaint Letter.

CERTIFICATE OF SERVICE

I hereby certify that on the 13th day of March, 2017, a copy of the FIRST AMENDED COMPLAINT ANSWER AND AFFRIMATIVE DEFENSES; AND COUNTERCLAIM was served on the Plaintiff's attorney, whose name and address are:

Charles C. Rainey, ESQ.
HAMRICK & EVANS LLP
7670 W. Lake Mead Blvd., Ste. 140
Las Vegas, Nevada 89128



Brian Kabala